

Exhibit A

E-FILED
10/31/2023 9:58 AM
Clerk of Court
Superior Court of CA,
County of Santa Clara
23CV424996
Reviewed By: R. Walker

JASON M. WUCETICH (STATE BAR NO. 222113)
jason@wukolaw.com
DIMITRIOS V. KOROVILAS (STATE BAR NO. 247230)
dimitri@wukolaw.com
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201

Attorneys for Plaintiff
KATHY VASQUEZ, individually and
on behalf of all others similarly situated

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SANTA CLARA

CASE NO. **23CV424996**

KATHY VASQUEZ, individually and on behalf
of all others similarly situated,

Plaintiff,

-v-

23ANDME, INC.,

Defendant.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff Kathy Vasquez (“Plaintiff”), on behalf of herself and all others similarly
2 situated, brings this class Action Complaint (the “Action”) against Defendant 23andMe, Inc.
3 (“23andMe” or “Defendant”), and alleges the following upon information and belief, except as
4 to allegations concerning Plaintiff herself and her actions, which are alleged upon personal
5 knowledge:

6 **I. INTRODUCTION**

7 1. Plaintiff seeks to hold Defendant responsible for the harm it has caused and will
8 continue to cause to Plaintiff and millions of other similarly situated person as a result of
9 Defendant’s inadequate data security policies and practices, which allowed unidentified third
10 parties to download and sell extraordinarily targeted and sensitive personally identifiable
11 information (PII) of Plaintiff and other class members on the Dark Web, including their names,
12 cities and states of residence, genders, years of birth, 23andMe account information, as well as
13 detailed information about Plaintiff and Class Members’ genomics, DNA profile, and
14 information about their ancestry and ethnicity (the “Data Breach”).

15 2. While Defendant has publicly stated that the Data Breach was a result of
16 compromised user credentials whereby attackers gained access to data through passwords that
17 users had reused from other websites that were hacked, that explanation is only a fraction of the
18 story. There should have been no way for any unauthorized third parties to be able to download
19 the sensitive PII of any individuals without being detected and stopped. However, Defendant
20 allowed the sensitive PII *of millions of users* to be downloaded and offered for sale on a Dark
21 Web hacker forum all without Defendant ever detecting this activity. Indeed, Defendant clearly
22 had no security policies or practices in place to detect or stop this Data Breach from occurring.

23 3. Companies entrusted with sensitive personal information, such as Defendant who
24 was entrusted with the detailed genetic information of its customers, should do everything
25 possible to protect against cybersecurity incidents, such as the Data Breach. While Defendant
26 clearly did not maintain adequate cybersecurity policies and practices, Defendant marketed
27 itself as operating a privacy and security-centric business practices. Specifically, Defendant
28

1 represented on its main privacy webpage that “we’re doing everything in our power to keep
2 your personal data safe.”¹

3 4. Moreover, Defendant specifically informed prospective customers that “your
4 personally identifiable information (such as your name and email) is stored in in a separate
5 database from your genetic data so that no one but you (when you use your username and
6 password) can connect the dots between the two”[sic] and that, as a result, “even if someone
7 gained access to one of these databases, they could not connect your identity to your genetic
8 data, or vice versa.”² Defendant also represented to prospective customers that “[w]e meet the
9 highest industry standards for data security. Our information security management system
10 received certification under the globally recognized ISO/IEC 27001:2013, 27018 & 27701
11 standards after an extensive security audit.”³

12 5. Indeed, the Data Breach shows these representations to be false. The hacker(s)
13 here were not only able to access genetic and genomic data for millions of people but, were also
14 able to associate this stolen sensitive PII with the names, years of birth, cities and states of
15 residence, genders, and 23andMe account information of these affected individuals.

16 6. In addition to violating its specific representations to consumers, Defendant’s
17 actions constitute a clear failure to take and implement adequate and reasonable measures to
18 ensure that Plaintiff’s and Class Members’ PII was safeguarded, failing to take available steps
19 to prevent unauthorized disclosure of data, and failing to follow applicable, required, and
20 appropriate protocols, policies, and procedures regarding the encryption of data, even for
21 internal use. Plaintiff and Class Members have a continuing interest in ensuring that their
22 information is and remains safe and are entitled to injunctive and other equitable relief.

23
24
25
26 ¹ See 23andMe “Privacy and Data Protection” webpage, <https://www.23andme.com/privacy/>
(last accessed on October 18, 2023).

27 ² *Id.*

28 ³ *Id.*

II. PARTIES

7. Plaintiff Kathy Vasquez is a resident and citizen of California and has been a 23andMe customer since approximately 2021.

8. Defendant 23andMe, Inc. is Delaware corporation with its principal place of business located at 223 N. Mathilda Avenue, Sunnyvale, California 94086.

III. JURISDICTION AND VENUE

9. This Court has general personal jurisdiction over Defendant because, at all relevant times, Defendant is a corporation registered to do business in California with the California Secretary of State. Further, it has had systematic and continuous contacts with the State of California. Defendant is based in Sunnyvale, California, and regularly contracts with a multitude of businesses and organizations in California.

10. Furthermore, this Court has specific personal jurisdiction over Defendant because the claims in this action stem from its specific contacts with the State of California — namely, Defendant’s collection, maintenance, and processing of the personal data of Californians in connection with its business, Defendant’s failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent cybersecurity attack and security breach of such data on or around October 6, 2023 that resulted from Defendant’s failures.

11. Venue is proper in the County of Santa Clara in accordance with Code of Civil Procedure § 395.5 because the alleged wrongs occurred in this county and Defendant conducts business and has its corporate headquarters in Santa Clara County.

IV. STATEMENT OF FACTS

A. Defendant’s Business

12. Defendant is a consumer genetics company founded with the mission “to help people access, understand, and benefit from the human genome.”⁴ Defendant provides

⁴https://investors.23andme.com/?_gl=1*ltxxa*_ga*MTcxMDQzMTYwNC4xNjk3MDQ4MDMx*_ga_G330GF3ZFF*MTY5NzQ5NDM0OS4yLjEuMTY5NzQ5NDM4OC4wLjAuMA.. (last visited Oct. 16, 2023).

consumers with DNA analysis, genetic healthcare information, and genetic ancestry analysis services.

13. In order to use Defendant's services, consumers use a saliva collection kit that Defendant mails to them to collect their saliva at home and mail it back to Defendant's lab in a pre-paid package. Within an average of 3-4 weeks, Defendant analyzes the DNA in the individual's saliva sample and provides detailed personalized reports on everything from the individual's personal genetic health risks and carrier status for various diseases, to the individual's detailed genomics and ancestry profile.⁵

14. The information contained in the individual's genome is then summarized in a report prepared by Defendant which provides an extraordinarily detailed—and intimate—snapshot of the individual's health risks and disease profile. In addition to detailed information about the individual's health and disease profile, the report prepared by Defendant also contains detailed sensitive information about the individual's ethnic and ancestral background.

15. Defendant also provides pharmacogenetics reports that detail how "[individual]' genetics can influence how [the individuals] process certain medications."⁶ Specifically, one type of report Defendant makes available to consumers is called a "Simvastatin Medication Insight report," which provides an analysis of how individuals respond to simvastatin, a commonly-proscribed statin used to lower cholesterol in the blood and reduce the risk of heart attacks, strokes, and heart disease. The report also indicates whether they have an increased chance of experiencing side effects.⁷

B. Defendant's Representations About Security and Privacy

16. Consumers today have dozens of choices for genetic testing services, with some of the leading offerings being AncestryDNA, MyHeritage, Living DNA, FamilyTreeDNA,

⁵ <https://www.23andme.com/genetic-science/> (last visited Oct. 16, 2023).

⁶ See https://www.23andme.com/topics/pharmacogenetics/slco1b1/?_gl=1*1jvwy6o*_ga*MTcxMDQzMtYwNC4xNjk3MDQ4MDMx*_ga_G330GF3ZFF*MTY5NzU2MjU0My4zLjEuMTY5NzU2MzU3MC4wLjAuMA (last visited Oct. 16, 2023).

⁷ *Id.*

1 Nebula Genomics, SelfDecode, and My Toolbox Genomics. In seeking to distinguish itself
2 from the many other genetic testing services available for consumers, Defendant touts its
3 privacy and security practices.

4 17. For example, Defendant tells consumers, in no uncertain terms on the company's
5 primary "About" webpage, that "[y]ou are in control of your DNA and your data," and that
6 "[w]e believe you should have a safe place to explore and understand your genes. That's why
7 Privacy and Security are woven into everything we do."⁸

8 18. On Defendant's Privacy and Data Protection webpage, Defendant elaborates on
9 its practices, saying that "When you explore your DNA with 23andMe, you entrust us with
10 important personal information. That's why, since day one, protecting your privacy has been
11 our number one priority. We're committed to providing you with a safe place where you can
12 learn about your DNA knowing your privacy is protected."⁹ Defendant also states that "[w]e
13 meet the highest industry standards for data security. Our information security management
14 system received certification under the globally recognized ISO/IEC 27001:2013, 27018 &
15 27701 standards after an extensive security audit."¹⁰

16 19. In addition to its claims about privacy protections, Defendant claims to
17 understand and prioritize data security and touts its data security practices as a selling point. For
18 example, Defendant represents that "Your data is fiercely protected by security practices that
19 are regularly reviewed and updated. Your genetic information deserves the highest level of
20 security, because without security, you can't have privacy. 23andMe employs software,
21 hardware, and physical security measures to protect your data." Defendant also represents that
22 "while no security standard or system is bulletproof, we're doing everything in our power to
23 keep your personal data safe."¹¹

24
25
26 ⁸ See <https://www.23andme.com/about/> (last visited Oct. 16, 2023).

27 ⁹ <https://www.23andme.com/privacy/> (last visited Oct. 16, 2023).

28 ¹⁰ *Id.*

¹¹ *Id.*

20. Defendant has even claimed to understand the need to stay “a step ahead of hackers,” and represented to current and potential customers that it does stay a step ahead of hackers:

“What do you do to stay a step ahead of hackers? We take multiple steps. First of all, third-party security experts regularly conduct audits and assessments of our systems, ensuring we will never let our guard down. We encrypt all sensitive information, both when it is stored and when it is being transmitted, so that we make it difficult for potential hackers to gain access.”¹²

21. To assure any consumers who may still be concerned about sharing their intimate personal and detailed genetic information with Defendant, Defendant represented that personally identifiable information such as name and email could never be connected with genetic data:

“Anything else you can tell me to put my mind at ease?

Rest assured that your personally identifiable information (such as your name and email) is stored in in a separate database from your genetic data so that no one but you (when you use your username and password) can connect the dots between the two. That means even if someone gained access to one of these databases, they could not connect your identity to your genetic data, or vice versa.”¹³

22. Consumers, including Plaintiff and Class Members, relied on Defendant’s representations in choosing Defendant’s services and in agreeing to turn over their DNA, and money, to Defendant.

23. Instead of upholding its promises to current and potential customers, Defendant failed to implement and provide adequate data security policies, measures, and procedures to prevent the unauthorized third-party hackers from downloading the PII, including the sensitive PII of millions of users. Indeed, while Defendant assured consumers that “even if someone gained access to [a genetic database] they could not connect your identity to your genetic data, or vice versa,”¹⁴ the Data Breach has showed that representation to false and that Plaintiff’s and

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

Class Members’ genetic information was easily stolen, sold, and associated with their names and identifying information by the hackers.

C. The Data Breach

24. In an announcement posted to 23andMe’s website on October 6, 2023 (the “Announcement”), 23andMe explains:

“We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users’ authorization.

After learning of suspicious activity, we immediately began an investigation. While we are continuing to investigate this matter, we believe threat actors were able to access certain accounts in instances where users recycled login credentials – that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked,

We believe the treat actor may have then, in violation of our Terms of Service, accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users’ DNA Relatives profiles, to the extent a user opted into that service.”¹⁵

25. Defendant’s Announcement failed to provide additional information, including the number of affected individuals or the specific types of information available. However, numerous sources, including some from the Dark Web, show that at least 999,998 individuals were affected by the Data Breach, including Plaintiff and Class Members, that likely more than 7 million users are implicated, and that the hacker clearly targeted individuals of Ashkenazi Jewish decent.

26. On or around October 3, 2023, the hacker responsible for the cyberattack posted on a Dark Web hacker forum claiming to have data for 7 million users—i.e., half of the members of 23andMe—including information about origin estimation, phenotype and health information. To validate the hacker’s claim to have this extremely sensitive genetic data, the hacker posted a spreadsheet entitled “Ashkenazi DNA Data of Celebrities” that contained the

¹⁵ See <https://blog.23andme.com/articles/addressing-data-security-concerns> (last visited October 18, 2023).

names and sensitive PII, including genetic information, for 999,998 individuals, including Plaintiff.

27. The PII in the sample spreadsheet posted online includes the name, gender, birth year, profile_id, account_id, location, and ancestral background information of approximately one million individuals of Ashkenazi Jewish decent. It also includes the Y-chromosome haplogroup for all male individuals listed and the mitochondrial DNA haplogroup for all of the listed individuals. These haplogroups provide a specific identification of the ancestral/genetic group that the individuals fall into and can be used to understand not only the specific ancestral lineage(s) the individual belongs in but also likely health-and disease-affecting genetic mutations the individual is likely to possess.

28. In addition to the spreadsheet labeled as containing “Ashkenazi DNA,” reports indicate that the 23andMe-derived genetic data of more than 300,000 individuals of Chinese heritage has already been disclosed.¹⁶

D. Defendant Violated Its Obligations to Plaintiff and Class Members

29. The Data Breach exposed Defendant’s inadequate cybersecurity and privacy practices as woefully insufficient. While Defendant’s announcement states that the information is information the individuals “opted into sharing through [Defendant’s] DNA Relatives feature,” Plaintiff and Class Members never opted into having this sensitive PII shared with the any unauthorized individuals, and certainly not cybercriminals.

30. More fundamentally, no company entrusted with such intimate personal information, such as Defendant, should have allowed a bad actor to abuse a feature meant to allow people to find and connect with their relatives in order to download the PII of millions of users. Any adequate cybersecurity protocol would have detected the hacker’s viewing and exfiltration of a few dozen people’s PII and alerted the company and/or cut off access. However, Defendant had no such protections and allowed the actor to exfiltrate the information of more than half of Defendant’s customers without being caught.

¹⁶ See <https://therecord.media/scraping-incident-genetic-testing-site> (last visited Oct. 18, 2023).

1 31. Indeed, the fact that Defendant only announced the Data Breach four days after
2 the hacker posted the stolen PII on a hacking forum suggests that Defendant only “learned” of
3 the Data Breach after the hacker posted, and sold, the information to the Dark Web and not
4 through any security alerts or detectors on Defendant’s systems.

5 32. As a direct result of Defendant’s failure to secure and safeguard the sensitive
6 information of customers that entrusted them to do so, all of this sensitive PII is in the hands of
7 cybercriminals. In fact, for the 999,998 Ashkenazi Jewish individuals and roughly 300,000
8 Chinese individuals, including Plaintiff, whose sensitive PII was already posted, the PII is now
9 in the hands of cybercriminals and is readily available to download by anyone with access to the
10 hacking forum.

11 33. At all relevant times, Defendant had a duty to Plaintiff and Class Members by
12 properly securing their PII, encrypt and maintain such information using industry standard
13 methods, train its employees, utilize available technology to defend its systems from invasion,
14 act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly
15 notify Plaintiff and Class Members when Defendant became aware that their PII may have been
16 compromised.

17 34. Defendant’s duty to use reasonable security measures arose as a result of the
18 special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class
19 Members, on the other hand. The special relationship arose because Plaintiff and the Members
20 of the Class relied on Defendant to secure their PII when they entrusted Defendant with the
21 information required to obtain Defendant’s services.

22 35. Defendant had the resources necessary to prevent the Data Breach but neglected
23 to adequately invest in adequate security measures, despite its obligation to protect customers’
24 PII. Accordingly, Defendant breached its common law, statutory, and other duties owed to
25 Plaintiff and Class Members.
26
27
28

36. Defendant owed a non-delegable duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information against unauthorized access and disclosure.

37. In fact, as detailed above, Defendant's failure to implement and maintain adequate security measures also violated Defendant's representations and promises to its current and prospective customers, on which Plaintiff and Class Members relied in choosing to (i) provide their genetic information to Defendant, (ii) allow Defendant to analyze their DNA to generate summaries of their health and ancestry-related genetics, and (iii) pay Defendant for such services.

38. As a result of the Data Breach, Plaintiff and Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, lost money paid to Defendant, and the loss of, and diminution in, value of their PII.

39. In addition, Plaintiff's and Class Members' sensitive PII, while compromised and taken by unauthorized third parties, also remains in Defendant's possession. Without additional safeguards and independent review and oversight, it remains vulnerable to future cyberattacks and theft.

40. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect victims' PII.

41. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant and entities like it, and Defendant was thus on notice that failing to take steps necessary to secure the PII against those risks left that property in a dangerous condition and vulnerable to theft. Defendant was further on notice of the severe consequences that would result to Plaintiff and Class Members from its failure to safeguard their PII.

42. Defendant failed to properly monitor the computer network and systems that stored the PII. Instead, had Defendant properly monitored its computer network and systems, it would have discovered the intrusion sooner and could have cut off access to the hacker(s) thereby mitigating the impact of the attack, as opposed to letting cyberthieves roam freely in Defendant's network for an unknown period of time.

43. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

44. Plaintiff and Class Members will incur out of pocket costs for undertaking protective measures to deter and detect identity theft.

45. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

46. Plaintiff seeks remedies including, but not limited to, actual damages, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the Class.

E. Defendant Failed to Comply with FTC Guidelines

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

48. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on

1 computer networks; understand their network’s vulnerabilities; and implement policies to
2 correct any security problems.¹⁷

3 49. The guidelines also recommend that businesses use an intrusion detection system
4 to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating
5 someone is attempting to hack the system; watch for large amounts of data being transmitted
6 from the system; and have a response plan ready in the event of a breach.¹⁸

7 50. The FTC further recommends that companies limit access to sensitive data;
8 require complex passwords to be used on networks; use industry-tested methods for security;
9 monitor for suspicious activity on the network; and verify that third-party service providers
10 have implemented reasonable security measures.

11 51. The FTC has brought enforcement actions against businesses for failing to
12 adequately and reasonably protect customer data, treating the failure to employ reasonable and
13 appropriate measures to protect against unauthorized access to confidential consumer data as an
14 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),
15 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must
16 take to meet their data security obligations.

17 52. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits “unfair . . . practices in or
18 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or
19 practice by businesses, such as Defendant, of failing to use reasonable measures to protect
20 personal, private Information. The FTC publications and orders described above also form part
21 of the basis of Defendant’s duty in this regard.

22 53. Defendant’s failure to employ reasonable and appropriate measures to protect
23 against unauthorized access to Plaintiff’s and Class Members’ PII or to comply with applicable
24

25
26 ¹⁷ See *Protecting Personal Information: A Guide for Business*, Federal Trade Commission
27 (2016), available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
28 0136_proteting-personal-information.pdf (last visited Oct. 17, 2023).

¹⁸ *Id.*

1 industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15
2 U.S.C. § 45.

3 54. Defendant was at all times fully aware of its obligation to protect the Private
4 Information of its customers, Defendant was also aware of the significant repercussions that
5 would result from its failure to do so. Accordingly, Defendant's conduct was particularly
6 unreasonable given the nature and amount of PII it obtained and stored and the foreseeable
7 consequences of the immense damages that would result to Plaintiff and the Class.

8 **F. Plaintiff Kathy Vasquez**

9 55. Plaintiff Kathy Vasquez is, and at all times relevant, has been a resident and
10 citizen of California. Plaintiff received two emails from Defendant on or around October 12,
11 2023, notifying her that her information was exposed in the Data Breach.

12 56. Plaintiff provided her PII to Defendant directly in order to obtain ancestry tracing
13 and genomic services from Defendant.

14 57. Plaintiff paid Defendant money in exchange for these services.

15 58. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff
16 has never knowingly transmitted unencrypted sensitive PII over the internet or any other
17 unsecured source.

18 59. As detailed above, Plaintiff received two emails directly from Defendant
19 confirming that her PII had been improperly accessed and/or obtained by unauthorized third
20 parties while in possession of Defendant.

21 60. The Data Breach email indicated that, while the investigation is ongoing,
22 Defendant believes that a threat actor was able to access certain accounts in instances where
23 users employed identical login credentials but does not mention the specific types of PII being
24 affected.

25 61. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the
26 impact of the Data Breach after receiving the data breach notification email including but not
27 limited to researching the Data Breach; reviewing credit reports, financial account statements,
28

1 and/or medical records for any indications of actual or attempted identity theft or fraud;
2 switching her VPN provider; and researching and purchasing additional antivirus, Dark Web
3 monitoring, and/or credit monitoring services.

4 62. Since the Data Breach, Plaintiff has received increased email spam, increased
5 scammer telephone calls and increased scammer text messages. Her father and aunt were also
6 contacted and told Plaintiff had been kidnapped and demanded ransom.

7 63. Plaintiff has spent hours addressing the Data Breach and will continue to spend
8 valuable time for the remainder of her life, that she otherwise would have spent on other
9 activities, including but not limited to work and/or recreation.

10 64. Plaintiff suffered actual injury from having her PII compromised as a result of
11 the Data Breach including, but not limited to (a) damage to and diminution in the value of her
12 PII, a form of property that Defendant maintained belonging to Plaintiff; (b) violation of her
13 privacy rights; (c) the theft of her PII; (d) lost money paid to Defendant and the lost benefit of
14 the bargain in Defendant's failure to comply with its obligations and representations, (e) the
15 out-of-pocket costs of purchasing additional identity theft protection, antivirus, Dark Web
16 monitoring, and/or credit monitoring software; and (f) present, imminent and impending injury
17 arising from the increased risk of identity theft and fraud. In fact, because her genetic data was
18 impacted, and because her PII was sold and exchanged on the Dark Web, Plaintiff faces this risk
19 for her lifetime.

20 65. As a result of the Data Breach, Plaintiff has also suffered emotional distress as a
21 result of the release of her PII, which she believed would be protected from unauthorized access
22 and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her
23 PII for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and
24 fraud, as well as the consequences of such identity theft and fraud resulting from the Data
25 Breach which was maliciously targeted at individuals that share Plaintiff's genetic heritage.

26 66. As a result of the Data Breach, Plaintiff anticipates spending considerable time
27 and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach.
28

1 In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of
2 identity theft and fraud for the remainder of her life.

3 **V. CLASS ALLEGATIONS**

4 67. Plaintiff brings this action on behalf of herself and all other similarly situated
5 persons pursuant to California Code of Civil Procedure § 382. Plaintiff seek to represent the
6 following class:

7 All citizens of the State of California whose personal information was compromised in or
8 as a result of the data breach of Defendant announced on or around October 6, 2023.

9 68. Excluded from the Classes are the following individuals and/or entities:
10 Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors and any entity
11 in which Defendant has a controlling interest, all individuals who make a timely election to be
12 excluded from this proceeding using the correct protocol for opting out, any and all federal,
13 state or local governments, including but not limited to its departments, agencies, divisions,
14 bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear
15 any aspect of this litigation, as well as their immediate family members.

16 69. In the alternative, Plaintiff requests additional subclasses as necessary based on
17 the types of PII that were compromised.

18 70. This action has been brought and may be maintained as a class action under
19 California Code of Civil Procedure § 382 because there is a well-defined community of interest
20 in the litigation and the proposed classes are ascertainable, as described further below:

- 21 a. Numerosity: A class action is the only available method for the fair and efficient
22 adjudication of this controversy. The members of the Class are so numerous that
23 joinder of all members is impractical, if not impossible. Plaintiff is informed and
24 believes and, on that basis, alleges that the total number of Class Members is at
25 least in the hundreds of thousands of individuals. Membership in the Class will
26 be determined by analysis of Defendant's records and/or through the records
27 made publicly available by the bad actor(s).

1 b. Commonality: Plaintiff and the Class Members share a community of interest in
2 that there are numerous common questions and issues of fact and law which
3 predominate over any questions and issues solely affecting individual members,
4 including, but not necessarily limited to:

- 5 i. Whether Defendant had a legal duty to Plaintiff and the Class to exercise
6 due care in collecting, storing, using and/or safeguarding their PII;
- 7 ii. Whether Defendant knew or should have known of the susceptibility of
8 its data security systems to a data breach;
- 9 iii. Whether Defendant's security procedures and practices to protect its
10 systems were reasonable in light of the measures recommended by data
11 security experts;
- 12 iv. Whether Defendant's failure to implement adequate data security
13 measures allowed the Data Breach to occur;
- 14 v. Whether Defendant failed to comply with its own policies and applicable
15 laws, regulations and industry standards relating to data security);
- 16 vi. Whether Defendant adequately, promptly and accurately informed
17 Plaintiff and Class Members that their PII had been compromised;
- 18 vii. How and when Defendant actually learned of the Data Breach;
- 19 viii. Whether Defendant's conduct, including its failure to act, resulted in or
20 was the proximate cause of the breach of its systems, resulting in the loss
21 of the PII of Plaintiff and Class Members;
- 22 ix. Whether Defendant adequately addressed and fixed the vulnerabilities
23 which permitted the Data Breach to occur;
- 24 x. Whether Defendant engaged in unfair, unlawful or deceptive practices by
25 failing to safeguard Plaintiff's and Class Members' PII;
- 26 xi. Whether Plaintiff and Class Members are entitled to actual and/or
27 statutory damages and/or whether injunctive, corrective and/or
28

1 declaratory relief and/or an accounting is/are appropriate as a result of
2 Defendant's wrongful conduct;

3 xii. Whether Plaintiff and Class Members are entitled to restitution as a result
4 of Defendant's wrongful conduct.

5 c. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and
6 all members of the Class sustained damages arising out of and caused by
7 Defendant's common course of conduct in violation of law, as alleged herein.

8 d. Adequacy of Representation: Plaintiff in this class action is an adequate
9 representative of the Class in that Plaintiff has the same interest in the litigation
10 of this case as the Class Members, are committed to the vigorous prosecution of
11 this case and have retained competent counsel who are experienced in
12 conducting litigation of this nature. Plaintiff is not subject to any individual
13 defenses unique from those conceivably applicable to other Class Members or
14 the Class in their entirety. Plaintiff anticipates no management difficulties in this
15 litigation.

16 e. Superiority of Class Action: The damages suffered by individual Class Members
17 are significant but may be small relative to each member's enormous expense of
18 individual litigation. This makes or may make it impractical for members of the
19 Class to seek redress individually for the wrongful conduct alleged herein. Even
20 if Class Members could afford such individual litigation, the court system could
21 not. Should separate actions be brought or be required to be brought by each
22 individual member of the Class, the resulting multiplicity of lawsuits would
23 cause undue hardship and expense for the Court and the litigants. The
24 prosecution of separate actions would also create a risk of inconsistent rulings
25 which might be dispositive of the interests of other Class Members who are not
26 parties to the adjudications and/or may substantially impede their ability to
27 protect their interests adequately. Individualized litigation increases the delay
28

1 and expense to all parties and to the court system, presented by the case's
2 complex legal and factual issues. By contrast, the class action device presents far
3 fewer management difficulties and provides the benefits of single adjudication,
4 economy of scale and comprehensive supervision by a single court.

5 71. Class certification is proper because the questions raised by this Complaint are of
6 common or general interest affecting numerous persons, so it is impracticable to bring all Class
7 Members before the Court.

8 72. This class action is also appropriate for certification because Defendant has acted
9 or refused to act on grounds generally applicable to Class Members, thereby requiring the
10 Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class
11 Members and making final injunctive relief appropriate concerning the Classes in their
12 entirety. Defendant's policies and practices challenged herein apply to and affect Class
13 Members uniformly. Plaintiff's challenge of these policies and practices hinges on Defendant's
14 conduct concerning the Classes in their entirety, not on facts or law applicable only to Plaintiff.

15 **CAUSES OF ACTION**

16 **COUNT ONE** 17 **(Negligence)**

18 73. Each and every allegation of the preceding paragraphs is incorporated in this
19 Count with the same force and effect as though fully set forth herein.

20 74. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty
21 of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use
22 commercially reasonable methods to do so. Defendant took on this obligation upon accepting
23 and storing Plaintiff's and Class Members' PII on its computer systems and networks.

24 75. The duty Defendant owed Plaintiff and Class Members includes but is not
25 limited to (a) the duty to exercise reasonable care in obtaining, retaining, securing, safeguarding,
26 deleting and protecting the PII in its possession; (b) the duty to protect Plaintiff's and Class
27 Members' PII using reasonable and adequate security procedures and systems that were/are
28 compliant with industry-standard practices and/or its own representations; (c) the duty to

1 implement processes to detect the Data Breach quickly and to act on warnings about data
2 breaches timely; and (d) the duty to promptly notify Plaintiff and Class Members of any data
3 breach, security incident or intrusion that affected or may have affected their PII.

4 76. Defendant knew or should have known that the PII was private and confidential
5 and should be protected as private and confidential and, thus, Defendant owed a duty of care to
6 not subject Plaintiff and Class Members to an unreasonable risk of harm because they were
7 foreseeable and probable victims of any inadequate security practices.

8 77. Defendant knew or should have known of the risks inherent in collecting and
9 storing PII, the vulnerabilities of its data security systems and the importance of adequate
10 security. Defendant knew or should have known about numerous well-publicized data breaches,
11 including breaches dealing with genetic information of individuals.

12 78. Defendant knew or should have known that its data systems and networks did
13 not adequately safeguard Plaintiff's and Class Members' PII.

14 79. Because Defendant knew that a breach of its systems could damage numerous
15 individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect
16 its data systems and the PII stored thereon.

17 80. Only Defendant was in the position to ensure that its systems and protocols were
18 sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

19 81. Defendant breached its duties to Plaintiff and Class Members by failing to
20 provide fair, reasonable, or adequate computer systems and data security practices to safeguard
21 their PII. This breach of duty includes but is not limited to (a) failing to implement computer
22 systems and data security practices to detect the intrusion and downloading of PII for millions
23 of Defendant's customers; (b) failing to timely and accurately disclose that Plaintiff's and Class
24 Members' PII had been improperly acquired or accessed; (c) failing to provide adequate
25 supervision and oversight of the PII with which it was and is entrusted, in spite of the known
26 risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party
27 to gather Plaintiff's and Class Members' PII, misuse the PII and intentionally disclose it to
28

1 others without consent; (d) failing to adequately train its employees with respect to security
2 practices that would have prevented or mitigated the extent of the Data Breach; (e) failing to
3 adequately enforce security policies aimed at protecting Plaintiff's and Class Members' PII; and
4 (f) failing to implement processes to quickly detect data breaches, security incidents or
5 intrusions such as the Data Breach in question.

6 82. As a proximate and foreseeable result of Defendant's negligent conduct, Plaintiff
7 and Class Members have suffered damages and are at imminent risk of additional harm and
8 damages (as alleged above).

9 83. Further, by explicitly failing to provide timely and clear notification of the Data
10 Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from
11 taking meaningful, and proactive steps to secure their PII.

12 84. There is a close causal connection between Defendant's failure to implement
13 security measures to protect Plaintiff's and Class Members' PII and the harm (or risk of
14 imminent harm suffered) by Plaintiff and Class Members. Plaintiff's and Class Members' PII
15 was accessed as the proximate result of Defendant's failure to exercise reasonable care in
16 safeguarding such PII by adopting, implementing, and maintaining appropriate security
17 measures.

18 85. Defendant's wrongful actions, inactions, and omissions constituted (and continue
19 to constitute) common law negligence.

20 86. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
21 Members have suffered and will continue to suffer injury, including but not limited to (a)
22 damage to and diminution in the value of their PII, a form of property that Defendant
23 maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c)
24 (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and
25 the lost benefit of the bargain in Defendant's failure to comply with its obligations and
26 representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of
27
28

1 the Data Breach; and (f) the present, imminent and impending injury arising from the increased
2 risk of identity theft and fraud.

3 87. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
4 Members have suffered and will continue to suffer other forms of injury and/or harm, including
5 but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-
6 economic losses.

7 88. Additionally, as a direct and proximate result of Defendant's negligence,
8 Plaintiff and Class Members have suffered and will continue to suffer the continued risks of
9 exposure of their PII, which remains in Defendant's possession and is subject to further
10 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
11 measures to protect PII in its continued possession.

12 **COUNT TWO**
13 **(Breach of Implied Contract)**

14 89. Each and every allegation of the preceding paragraphs is incorporated in this
15 Count with the same force and effect as though fully set forth herein.

16 90. Through their course of conduct, Defendant, Plaintiff, and Class Members
17 entered into implied contracts for Defendant to implement data security adequate to safeguard
18 and protect the privacy of Plaintiff's and Class Members' PII.

19 91. Defendant required Plaintiff and Class Members to provide and entrust their PII
20 to it as a condition of obtaining Defendant's services.

21 92. Defendant solicited and invited Plaintiff and Class Members to provide their PII
22 as part of Defendant's regular business practices. Plaintiff and Class Members accepted
23 Defendant's offers and provided their PII to Defendant.

24 93. As a part of the agreement, as discussed above, Defendant specifically agreed
25 that it would provide security to detect and prevent data breaches and misuse of Plaintiff's and
26 Class Members' PII, to safeguard and protect such non-public information, and to keep such
27 information secure and confidential. Defendant also impliedly agreed to timely and accurately
28 notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

94. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII and money to Defendant, in exchange for, amongst other things, the protection of their PII.

95. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

96. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised because of the Data Breach.

97. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c) (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and the lost benefit of the bargain in Defendant's failure to comply with its obligations and representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of the Data Breach; and (f) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

COUNT THREE
(Breach of Implied Covenant of Good Faith and Fair Dealing)

98. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

99. Every contract has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

100. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

101. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII,

1 failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members, and
2 continued acceptance of PII and storage of other personal information after Defendant knew or
3 should have known of the security vulnerabilities of the systems that were exploited in the Data
4 Breach.

5 102. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff
6 and Class Members the full benefit of their bargains as originally intended by the parties,
7 thereby causing them injury in an amount to be determined at trial.

8 **COUNT FOUR**
9 **(Unjust Enrichment)**

10 103. Each and every allegation of the preceding paragraphs is incorporated in this
11 Count with the same force and effect as though fully set forth herein.

12 104. Plaintiff and Class Members conferred a monetary benefit on Defendant.
13 Specifically, they purchased goods and services from Defendant and in so doing provided
14 Defendant with their Private Information. In exchange, Plaintiff and Class Members should
15 have received from Defendant the goods and services that were the subject of the transaction
16 and have their PII protected with adequate data security.

17 105. Defendant knew that Plaintiff and Class Members conferred a benefit which
18 Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and
19 Class Members for business purposes.

20 106. The amounts Plaintiff and Class Members paid for goods and services were used,
21 in part, to pay for use of Defendant's network and the administrative costs of data management
22 and security.

23 107. Under the principles of equity and good conscience, Defendant should not be
24 permitted to retain the money belonging to Plaintiff and Class Members, because Defendant
25 failed to implement appropriate data management and security measures that are mandated by
26 industry standards and by Defendant's own representations to Plaintiff and Class Members.
27
28

1 108. Defendant failed to secure Plaintiff's and Class Members' Private Information
2 and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members
3 provided.

4 109. Defendant acquired the PII through inequitable means in that it failed to disclose
5 the inadequate security practices previously alleged.

6 110. If Plaintiff and Class Members knew that Defendant had not reasonably secured
7 their PII, they would not have agreed to Defendant's services.

8 111. Plaintiff and Class Members have no adequate remedy at law.

9 112. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
10 Members have suffered and will continue to suffer injury, including but not limited to (a)
11 damage to and diminution in the value of their PII, a form of property that Defendant
12 maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c)
13 (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and
14 the lost benefit of the bargain in Defendant's failure to comply with its obligations and
15 representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of
16 the Data Breach; and (f) the present, imminent, and impending injury arising from the increased
17 risk of identity theft and fraud.

18 113. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
19 Members have suffered and will continue to suffer injury, including but not limited to (a)
20 damage to and diminution in the value of their PII, a form of property that Defendant
21 maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c)
22 (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and
23 the lost benefit of the bargain in Defendant's failure to comply with its obligations and
24 representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of
25 the Data Breach; and (f) the present, imminent, and impending injury arising from the increased
26 risk of identity theft and fraud.

114. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

115. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT FIVE
**(Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.*)**

116. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

117. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200 *et seq.* (“UCL”), prohibits any “fraudulent,” or “unfair” business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

118. By reason of Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, as described above, and the unauthorized disclosure of Plaintiff and Class Members' PII, Defendant engaged in unfair practices within the meaning of the UCL.

119. Defendant has violated the UCL by engaging in unfair business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of “unfair competition” as defined in the UCL with respect to the services provided to the Class.

120. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the PII of Plaintiff and Class Members has been compromised.

121. Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Class Members' PII also constitute "unfair" business acts and practices within the meaning the UCL in that Defendant's conduct was substantially injurious to Plaintiff and Class Members, offensive to public policy,

1 immoral, unethical, oppressive and unscrupulous, and the gravity of Defendant's conduct
2 outweighs any alleged benefits attributable to such conduct.

3 122. Defendant's business practices as alleged herein are wrongful and unfair
4 because, through the specific statements described above, Defendant is likely to mislead
5 consumers into believing that the PII they provided to Defendant will remain private and secure,
6 when in fact it has not been maintained in a private and secure manner, that Defendant would
7 employ computer systems and practices to prevent the access to and downloading of millions of
8 users' PII, when in fact it did not, and that Defendant would take proper measures to investigate
9 and remediate a data breach such as, when Defendant did not do so.

10 123. Plaintiff and Class Members suffered (and continue to suffer) injury in fact and
11 lost money or property as a direct and proximate result of Defendant's unfair competition and
12 violation of the UCL, including but not limited to the price received by Defendant for the
13 services, the loss of Plaintiff's and Class Members' legally protected interest in the
14 confidentiality and privacy of their Private Information, nominal damages, and additional losses
15 as described above.

16 124. Plaintiff, on behalf of the Class, seeks relief under the UCL, including, but not
17 limited to, restitution to Plaintiff and Class Members of money or property that Defendant may
18 have acquired by means of Defendant's unfair and fraudulent business practices, restitutionary
19 disgorgement of all profits accruing to Defendant because of Defendant's unfair business
20 practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc.
21 §1021.5), and injunctive or other equitable relief.

22 **COUNT SIX**
23 **(Violation of the California Consumer Privacy Act,**
24 **Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a)**
25 **By Plaintiff and the Class Against All Defendants)**

26 125. Plaintiff realleges and incorporates by reference the preceding paragraphs as
27 though fully set forth herein.
28

1 126. The California Consumer Privacy Act (“CCPA”), Cal. Civ. Code § 1798.150(a),
2 creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically
3 provides:

4 Any consumer whose nonencrypted and nonredacted personal information, as
5 defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section
6 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or
7 disclosure as a result of the business’s violation of the duty to implement and
8 maintain reasonable security procedures and practices appropriate to the nature of
the information to protect the personal information may institute a civil action for
any of the following:

9 (A) To recover damages in an amount not less than one hundred dollars
10 (\$100) and not greater than seven hundred and fifty (\$750) per consumer
per incident or actual damages, whichever is greater.

11 (B) Injunctive or declaratory relief.

12 (C) Any other relief the court deems proper.

13
14 127. Defendant is a “business” under § 1798.140(b) in that it is a corporation organized
15 for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of
16 \$25 million.

17 128. Plaintiff and class members are covered “consumers” under § 1798.140(g) in that
18 they are natural persons who are California residents.

19 129. The personal information of Plaintiff and class members at issue in this lawsuit
20 constitutes “personal information” under § 1798.150(a) and 1798.81.5, in that the personal
21 information Defendant collects and which was impacted by the cybersecurity attack includes an
22 individual’s first name or first initial and the individual’s last name in combination with one or
23 more of the following data elements, with either the name or the data elements not encrypted or
24 redacted: (i) Social security number; (ii) Driver’s license number, California identification card
25 number, tax identification number, passport number, military identification number, or other
26 unique identification number issued on a government document commonly used to verify the
27 identity of a specific individual; (iii) account number or credit or debit card number, in
28

1 combination with any required security code, access code, or password that would permit access
2 to an individual's financial account; (iv) medical information; (v) health insurance information;
3 (vi) unique biometric data generated from measurements or technical analysis of human body
4 characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific
5 individual; (vii) genetic data.

6 130. Defendant knew or should have known that its computer systems and data
7 security practices were inadequate to safeguard the Plaintiff's and class members' personal
8 information and that the risk of a data breach or theft was highly likely. Defendant failed to
9 implement and maintain reasonable security procedures and practices appropriate to the nature of
10 the information to protect the personal information of Plaintiff and the class. Specifically,
11 Defendant subjected Plaintiff's and class members' nonencrypted and nonredacted personal
12 information to an unauthorized access and exfiltration, theft, or disclosure as a result of the
13 Defendant's violation of the duty to implement and maintain reasonable security procedures and
14 practices appropriate to the nature of the information, as described herein.

15 131. As a direct and proximate result of Defendant's violation of its duty, the
16 unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and class members'
17 personal information included exfiltration, theft, or disclosure through Defendant's servers,
18 systems, and website, and/or the dark web, where hackers further disclosed Defendant's
19 customers' and their employees' personal information.

20 132. As a direct and proximate result of Defendant's acts, Plaintiff and class members
21 were injured and lost money or property, the loss of Plaintiff's and the class's legally protected
22 interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety,
23 nominal damages, and additional losses described above.

24 133. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be
25 required prior to an individual consumer initiating an action solely for actual pecuniary
26 damages." Accordingly, Plaintiff and the class by way of this complaint seek actual pecuniary
27 damages suffered as a result of Defendant's violations described herein. Plaintiff has issued
28

1 and/or will issue a notice of these alleged violations pursuant to § 1798.150(b) and intends to
 2 amend this complaint to seek statutory damages and injunctive relief upon expiration of the 30-
 3 day cure period pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b).

4 **COUNT SEVEN**

5 **(Violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, 6 By Plaintiff and the Class Against All Defendants)**

7 134. Plaintiff realleges and incorporates by reference the preceding paragraphs as
 8 though fully set forth herein.

9 135. Cal. Civ. Code § 1798.81.5 provides that “[i]t is the intent of the Legislature to
 10 ensure that personal information about California residents is protected. To that end, the purpose
 11 of this section is to encourage businesses that own, license, or maintain personal information
 12 about Californians to provide reasonable security for that information.”

13 136. Section 1798.81.5(b) further states that: “[a] business that owns, licenses, or
 14 maintains personal information about a California resident shall implement and maintain
 15 reasonable security procedures and practices appropriate to the nature of the information, to
 16 protect the personal information from unauthorized access, destruction, use, modification, or
 17 disclosure.”

18 137. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of
 19 this title may institute a civil action to recover damages.” Section 1798.84(e) further provides
 20 that “[a]ny business that violates, proposes to violate, or has violated this title may be enjoined.”

21 138. Plaintiff and members of the class are “customers” within the meaning of Civ.
 22 Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal
 23 information to Defendant.

24 139. The personal information of Plaintiff and the class at issue in this lawsuit
 25 constitutes “personal information” under § 1798.81.5(d)(1) in that the personal information
 26 Defendant collects and which was impacted by the cybersecurity attack includes an individual’s
 27 first name or first initial and the individual’s last name in combination with one or more of the
 28

1 following data elements, with either the name or the data elements not encrypted or redacted: (i)
2 Social security number; (ii) Driver's license number, California identification card number, tax
3 identification number, passport number, military identification number, or other unique
4 identification number issued on a government document commonly used to verify the identity of
5 a specific individual; (iii) account number or credit or debit card number, in combination with
6 any required security code, access code, or password that would permit access to an individual's
7 financial account; (iv) medical information; (v) health insurance information; (vi) unique
8 biometric data generated from measurements or technical analysis of human body characteristics,
9 such as a fingerprint, retina, or iris image, used to authenticate a specific individual; (vii) genetic
10 data.

11 140. Defendant knew or should have known that its computer systems and data
12 security practices were inadequate to safeguard the class's personal information and that the risk
13 of a data breach or theft was highly likely. Defendant failed to implement and maintain
14 reasonable security procedures and practices appropriate to the nature of the information to
15 protect the personal information of Plaintiff and the class. Specifically, Defendant failed to
16 implement and maintain reasonable security procedures and practices appropriate to the nature of
17 the information, to protect the personal information of Plaintiff and the class from unauthorized
18 access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and
19 the class's nonencrypted and nonredacted personal information to an unauthorized access and
20 exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement
21 and maintain reasonable security procedures and practices appropriate to the nature of the
22 information, as described herein.

23 141. As a direct and proximate result of Defendant's violation of its duty, the
24 unauthorized access, destruction, use, modification, or disclosure of the personal information of
25 Plaintiff and the class included hackers' access to, removal, deletion, destruction, use,
26 modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and
27
28

1 the class by the ransomware attackers and/or additional unauthorized third parties to whom those
2 cybercriminals sold and/or otherwise transmitted the information.

3 142. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and
4 the class were injured and lost money or property, including but not limited to the loss of
5 Plaintiff's and the class's legally protected interest in the confidentiality and privacy of their
6 personal information, nominal damages, and additional losses described above. Plaintiff seeks
7 compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

8 143. Moreover, the California Customer Records Act further provides: "A person or
9 business that maintains computerized data that includes personal information that the person or
10 business does not own shall notify the owner or licensee of the information of the breach of the
11 security of the data immediately following discovery, if the personal information was, or is
12 reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code §
13 1798.82.

14 144. Any person or business that is required to issue a security breach notification
15 under the CRA must meet the following requirements under §1798.82(d):

- 16 a. The name and contact information of the reporting person or business subject
17 to this section;
- 18 b. A list of the types of personal information that were or are reasonably believed to
19 have been the subject of a breach;
- 20 c. If the information is possible to determine at the time the notice is provided, then
21 any of the following:
- 22 i. the date of the breach,
- 23 ii. the estimated date of the breach, or
- 24 iii. the date range within which the breach occurred. The notification shall
25 also include the date of the notice;
- 26 d. Whether notification was delayed as a result of a law enforcement investigation, if
27 that information is possible to determine at the time the notice is provided;
- 28

- 1 e. A general description of the breach incident, if that information is possible to
2 determine at the time the notice is provided;
- 3 f. The toll-free telephone numbers and addresses of the major credit reporting
4 agencies if the breach exposed a social security number or a driver's license or
5 California identification card number;
- 6 g. If the person or business providing the notification was the source of the breach,
7 an offer to provide appropriate identity theft prevention and mitigation services, if
8 any, shall be provided at no cost to the affected person for not less than 12 months
9 along with all information necessary to take advantage of the offer to any person
10 whose information was or may have been breached if the breach exposed or may
11 have exposed personal information.

12 145. Plaintiff and class members were entitled to receive timely notice from
13 Defendant.

14 146. On information and belief, many class members affected by the breach, have not
15 received any notice at all from Defendant in violation of Section 1798.82(d).

16 147. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and class
17 members suffered incrementally increased damages separate and distinct from those simply
18 caused by the breaches themselves.

19 148. As a direct consequence of the actions as identified above, Plaintiff and class
20 members incurred additional losses and suffered further harm to their privacy, including but not
21 limited to economic loss, the loss of control over the use of their identity, increased stress, fear,
22 and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation
23 of the breach and effort to cure any resulting harm, the need for future expenses and time
24 dedicated to the recovery and protection of further loss, and privacy injuries associated with
25 having their sensitive personal, financial, and payroll information disclosed, that they would not
26 have otherwise incurred but for the data breach of Defendant, and are entitled to recover
27 compensatory damages according to proof pursuant to § 1798.84(b).
28

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. An order certifying the class pursuant to California Code of Civil Procedure § 382 and declaring that Plaintiff is the class representative and appointing Plaintiff's counsel as class counsel;
2. Permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. Compensatory, consequential, general, and nominal damages in an amount to be proven at trial;
4. Disgorgement and restitution of all earnings, profits, compensation, and benefits received as a result of the unlawful acts, omissions, and practices described herein;
5. Punitive, exemplary, and/or trebled damages to the extent permitted by law;
6. Plaintiff intends to amend this complaint to seek statutory damages upon expiration of the 30-day cure period pursuant to Cal. Civ. Code § 1798.150(b);
7. A declaration of right and liabilities of the parties;
8. Costs of suit;
9. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code § 1021.5;
10. Pre- and post-judgment interest at the maximum legal rate;
11. Distribution of any monies recovered on behalf of members of the class or the general public via fluid recovery or *cy pres* recovery where necessary and as applicable to prevent Defendant from retaining the benefits of their wrongful conduct; and

///

1 12. Such other relief as the Court deems just and proper.

2 Dated: October 31, 2023

3 WUCETICH & KOROVILAS LLP

4 

5 By: _____

6 Jason M. Wucetich
7 Attorneys for Plaintiff Kathy Vasquez,
8 individually and on behalf of
9 all others similarly situated
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the class, hereby demands a trial by jury on all issues of fact or law so triable.

Dated: October 31, 2023

WUCETICH & KOROVILAS LLP

By: 

Jason M. Wucetich
Attorneys for Plaintiff Kathy Vasquez,
individually and on behalf of
all others similarly situated

Exhibit B

1 Mark N. Todzo (Bar No. 168389)

2 **LEXINGTON LAW GROUP**

3 503 Divisadero Street

4 San Francisco, CA 94117

5 Telephone: 415-913-7800

6 Facsimile: 415-759-4112

7 mtodzo@lexlawgroup.com

8 *Attorneys for Plaintiff*

9 [Additional Counsel on Signature Page.]

10 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**

11 **COUNTY OF SAN FRANCISCO**

12 MARJORIE MORGENSTERN on Behalf of
13 Herself and All Others Similarly Situated,

14 Plaintiff,

15 v.

16 23ANDME HOLDING CO. and 23ANDME,
17 INC.,

18 Defendants.

No.

CLASS ACTION

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff Marjorie Morgenstern (“Plaintiff”), on behalf of herself and all others similarly
 2 situated, files this Complaint against Defendants 23andMe Holding Co. and 23andMe, Inc.
 3 (“23andMe” or “Defendant”). The following allegations are based upon Plaintiff’s personal
 4 knowledge with respect to herself and her own acts and upon information and belief as to all other
 5 matters following her and her counsel’s investigation.

6 INTRODUCTION

7 1. 23andMe hails itself as the “pioneer[]” of direct-to-consumer genetic testing and
 8 boasts that it has the “premier database of genetic and phenotypic information crowdsourced from
 9 its millions of customers” capable of providing “personalized information about [consumers’]
 10 genetic health risks, ancestry, and traits.”¹

11 2. 23andMe knowingly collects and stores troves of personally identifiable
 12 information (“PII”) and personal genetic and health information (“PGI”) and has a corresponding
 13 duty to implement and maintain reasonable security measures to keep that data secure. PII and
 14 PGI is property owned by Plaintiff and members of the Class that was shared with 23andMe for a
 15 limited purpose with the understanding that 23andMe would implement and maintain reasonable
 16 data security measures adequate to protect PII and PGI.

17 3. “[G]enetic information is inherently identifiable. . . .”² Unlike other types of
 18 personal information like financial information or Social Security Numbers, genetic information
 19 is immutable. “Once an individual’s genetic data is breached it can no longer be protected.”³
 20 Because genetic data is tied “intrinsically to our identity. . . genetic data breaches can have long-
 21
 22
 23

24 ¹ 23andMe Holding Co., Annual Report (Form 10-K) (March 31, 2022),
 25 <https://investors.23andme.com/static-files/536ba9a7-8a85-4b73-8b09-8215451089a0>.

26 ² Emily Christofides & Kieran O’Doherty, *Company Disclosure and Consumer Perceptions*
 27 *of the Privacy Implications of Direct-to-Consumer Genetic Testing*, NEW GENETICS AND SOCIETY
 35:2, 101-123 (2016).

28 ³ Sawaya, Sterling and Kenneally, Erin E. and Nelson, Demetrius and Schumacher, Garrett
 J., *Artificial Intelligence and the Weaponization of Genetic Data* at 13, SSRN (April 24, 2020).

1 lasting consequences and must be considered distinct from other types of data breaches.”⁴ Genetic
 2 data also identifies immutable relationships with others. With the genetic data of just 2% of a
 3 given population, researchers can “provide a third cousin match to nearly any person.”⁵

4 4. On October 6, 2023, 23andMe confirmed that “customer profile information” had
 5 been accessed “without the account users’ authorization,” and that a hacker had “obtained
 6 information from certain accounts, including information about users’ DNA Relatives profiles . . .”
 7 (the “Data Breach”).⁶

8 5. The PII and PGI compromised in the Data Breach has already been offered for sale
 9 on the dark web.

10 6. As a direct and proximate result of 23andMe’s failure to implement and maintain
 11 reasonable data security measures, Plaintiff and members of the Class have lost the ability to
 12 control the use and dissemination of their PII and PGI.

13 **PARTIES**

14 7. Plaintiff Marjorie Morgenstern is a citizen and resident of California.

15 8. Defendant 23andMe Holding Co. is a Delaware corporation with its headquarters
 16 and principal place of business located at 349 Oyster Point Blvd., South San Francisco, California
 17 94080.

18 9. Defendant 23andMe, Inc. is a Delaware corporation with its headquarters and
 19 principal place of business located at 223 N. Mathilda Ave., Sunnyvale, California 94086.

22
 23 ⁴ Sawaya, Sterling and Kenneally, Erin E. and Nelson, Demetrius and Schumacher, Garrett
 J., *Artificial Intelligence and the Weaponization of Genetic Data* at 13, SSRN (April 24, 2020).

24 ⁵ Yaniv Erlich, Tal Shor, Itsik Pe’er, Shai Carmi, *Identity Inference of Genomic Data using*
 25 *Long-Range Familial Searches*, Vol. 362 *SCIENCE* 690 (Oct. 11 2018) (“[W]e predict that with a
 26 database size of ~3 million US individuals of European descent (2% of the adults of this
 population), over 99% of the people of this ethnicity would have at least a single 3rd cousin match
 and over 65% are expected to have at least one 2nd cousin match.”).

27 ⁶ 23andMe, Addressing Data Security Concerns (Oct 6, 2023), [https://blog.23andme.com/](https://blog.23andme.com/articles/addressing-data-security-concerns)
 28 [\[https://web.archive.org/web/20231007110808/](https://web.archive.org/web/20231007110808/https://blog.23andme.com/articles/addressing-data-security-concerns)
[https://blog.23andme.com/articles/addressing-data-security-concerns\]](https://blog.23andme.com/articles/addressing-data-security-concerns).

VENUE

10. Venue is proper in this Court pursuant to California Code of Civil Procedure §395 because 23andMe resides in San Francisco County at the commencement of this action.⁷

JURISDICTION

11. This Court has subject-matter jurisdiction over this action pursuant to the California Constitution, Article VI § 10.

12. This Court has personal jurisdiction over Defendants pursuant to California Code of Civil Procedure §410.10 because 23andMe is headquartered in California, its principal place of business is in California, and it regularly conducts business in California.

FACTUAL BACKGROUND

A. 23andMe

13. 23andMe sells direct-to-consumer genetic testing kits to the public. To use 23andMe’s services, customers are required to provide a saliva sample that is subjected to single nucleotide polymorphism (“SNP”) genotyping. 23andMe identifies more than half a million SNPs from each saliva sample, which it uses to identify traits related to a person’s ancestry, wellness, health predispositions (including genetic health risks), and carrier status for inherited conditions.

14. 23andMe claims to have more than 14 million customers.⁸ According to 23andMe: “We receive and store a large volume of [PII], [PGI], and other data relating to our customers and patients. . . .”⁹

15. The PII and PGI that 23andMe collects undoubtedly has value. 23andMe claims that “insights” from customers’ PII and PGI “may highlight opportunities to develop a drug to treat

⁷ 23andMe Holding Co., Annual Report (Form 10-K) (March 31, 2022), <https://investors.23andme.com/static-files/536ba9a7-8a85-4b73-8b09-8215451089a0> (“Our corporate headquarters was previously located in Sunnyvale, California. . . . Effective April 1, 2022, we relocated our corporate headquarters to South San Francisco, California.”).

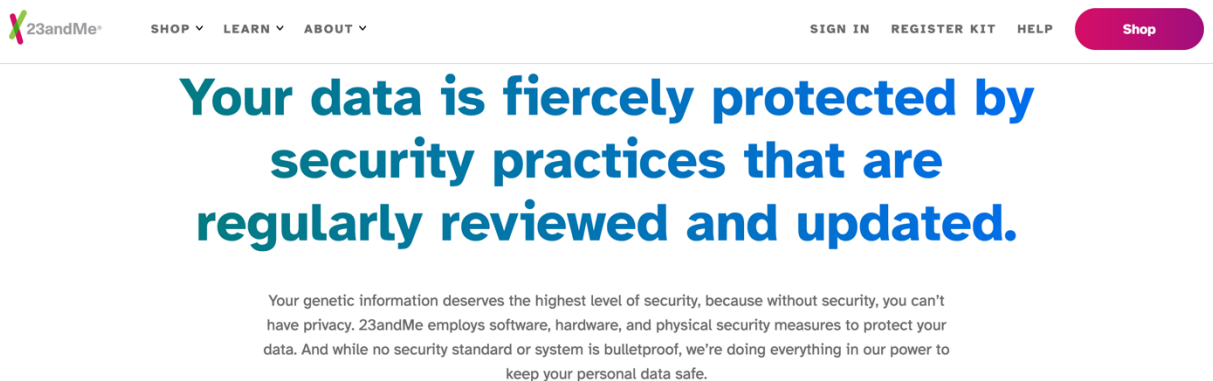
⁸ 23andMe for Medical Professionals, (Nov. 3, 2023), <https://medical.23andme.com/> [<https://web.archive.org/web/20231030132819/https://medical.23andme.com/>]

⁹ Form 10-K, *supra* n.7 at 72.

or cure a specific disease, and also provide information that customers can use to enhance their medical care and treatment.”¹⁰

16. Plaintiff and Class members reasonably expected that 23andMe would implement and maintain security measures adequate to protect their PII and PGI.

17. 23andMe tells customers that their “genetic information deserves the highest level of security, *because without security, you can’t have privacy.*”¹¹ [Emphasis added.]



Source: 23andMe¹²

18. 23andMe acknowledged that using its services required customers to “entrust us with important personal information.”

¹⁰ *Id.* at 10.

¹¹ Privacy and Data Protection, (Nov. 6, 2023), 23andMe, <https://www.23andme.com/privacy/> [https://web.archive.org/web/20231001063147/; <https://www.23andme.com/privacy/>].


¹² *Id.*

123andMe®

SHOP ▾LEARN ▾ABOUT ▾

SIGN INREGISTER KITHELP

Shop



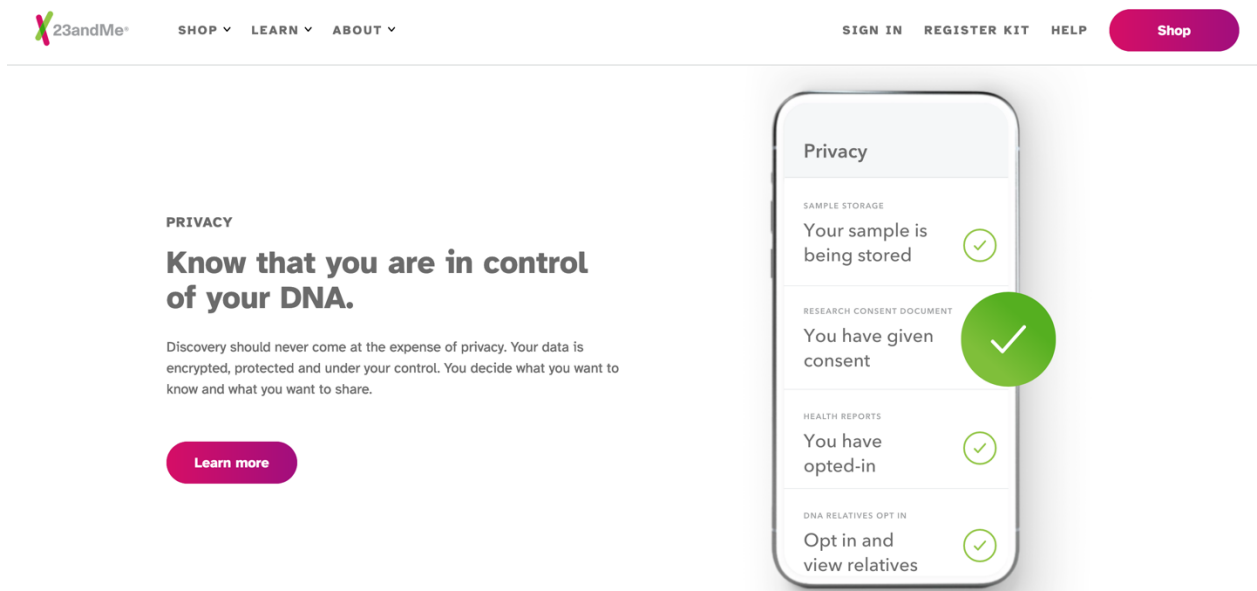
Your privacy comes first.

When you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected.

Source: 23andMe¹³

¹³ *Id.*

19. 23andMe promises customers that they are “in control” of their DNA, stating: “You decide what you want to know and what you want to share.”¹⁴



Source: 23andMe¹⁵

B. The Data Breach

20. On October 1, 2023, a hacker going by the handle “Golem”¹⁶ posted a link to what the hacker called: “The most valuable data you’ll ever see.”¹⁷ The link, which was posted on a “popular forum where stolen data is traded and sold,”¹⁸ contained a sample of nearly “20 million pieces of data” the hacker claimed to have exfiltrated from 23andMe. The data included “genomic

¹⁴ *Id.*

¹⁵ *Id.*

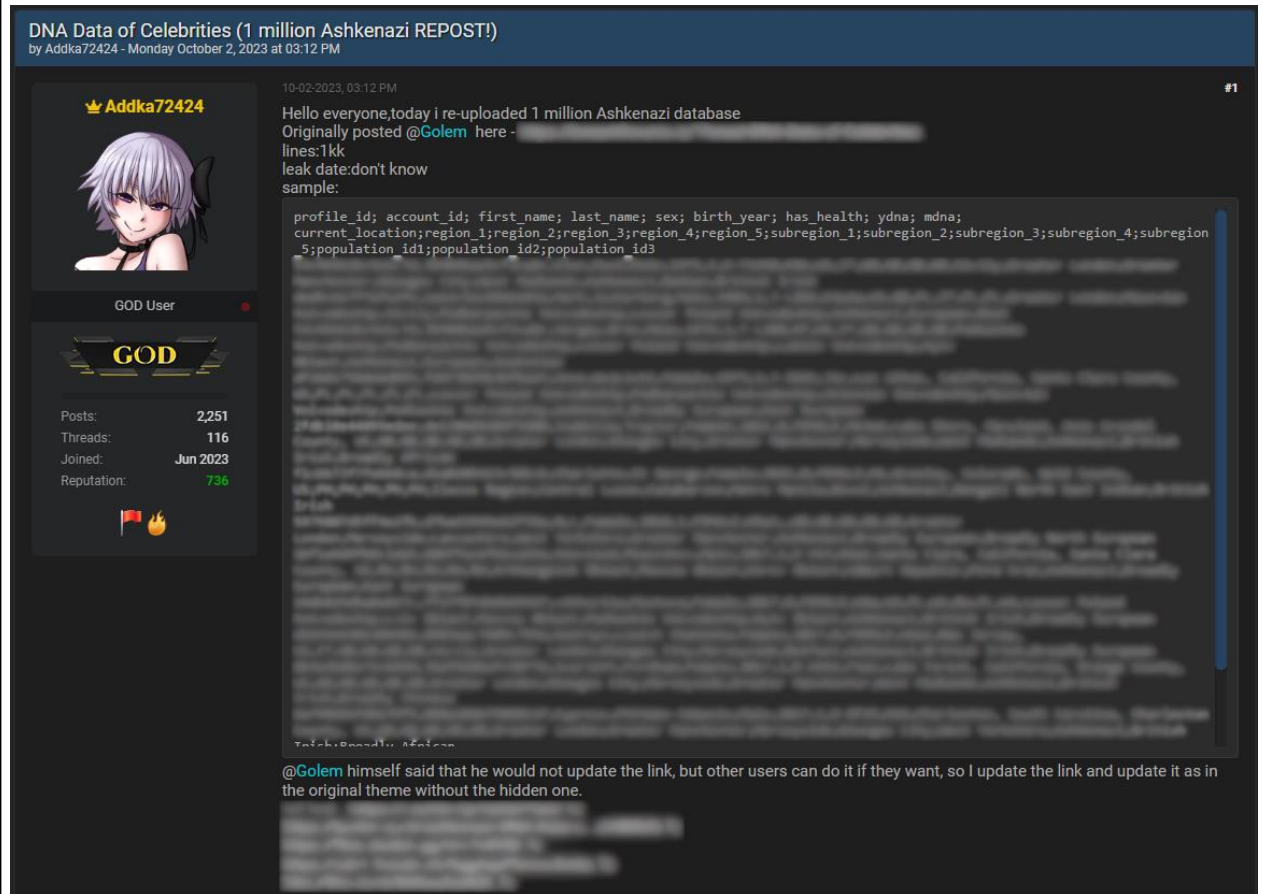
¹⁶ See also *Oxford English Dictionary*, s.v. “golem, n., sense 1,” July 2023, <https://doi.org/10.1093/OED/4113804198> (“[T]he golem was said to have been created by Rabbi Löw of Prague (d. 1609) in order to protect the city’s Jewish population from pogroms. However, the golem began to act independently of its master and so the rabbi returned it to dust.”).

¹⁷ AJ Vicens, *DNA testing service 23andMe investigating theft of user data*, CYBERSCOOP (Oct. 5, 2023), <https://cyberscoop.com/23andme-user-data-theft/>; see also *DNA Data of Celebrities*, BREACHFORUMS (Oct. 1, 2023), <https://breachforums.is/Thread-DNA-Data-of-Celebrities> [<https://webcache.googleusercontent.com/search?q=cache:cOVRhJGEU5kJ:https://breachforums.is/Thread-DNA-Data-of-Celebrities>].

¹⁸ Vicens, *supra* n.17.

ancestry data owned by 1 million Ashkenazi,” with “an extra 1 million Ashkenazi data available.”¹⁹ The hacker offered to sell the “[r]aw data” for a “fee” of “\$5 each.”²⁰

21. On October 2, 2023, the data was reposted along with a sample of the data compromised purportedly associated with 1 million individuals of Ashkenazi descent and 100,000 individuals of Chinese descent.



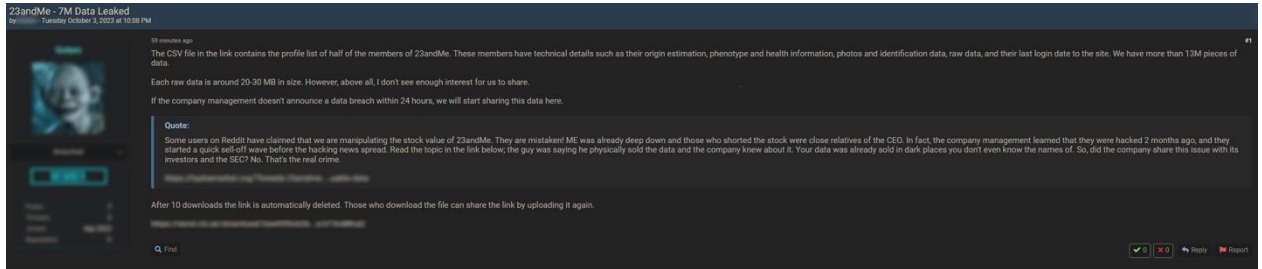
Source: Bleeping Computer²¹

¹⁹ *DNA Data of Celebrities*, BREACHFORUMS (Oct. 1, 2023), <https://breachforums.is/Thread-DNA-Data-of-Celebrities> [https://webcache.googleusercontent.com/search?q=cache:cOVRhJGEU5kJ: https://breachforums.is/Thread-DNA-Data-of-Celebrities].

²⁰ *Id.*

²¹ Bill Toulas, *Genetics firm 23andMe says user data stolen in credential stuffing attack*, BLEEPING COMPUTER (Oct. 6, 2023 11:48 AM), <https://www.bleepingcomputer.com/news/security/genetics-firm-23andme-says-user-data-stolen-in-credential-stuffing-attack/> [https://web.archive.org/web/20231006172221/https://www.bleepingcomputer.com/news/security/genetics-firm-23andme-says-user-data-stolen-in-credential-stuffing-attack/]; *DNA Data of Celebrities* (1 million Ashkenazi REPOST!), BreachForums (Oct. 2, 2023),

22. On October 3, 2023, the hacker again posted, claiming that the compromised data contained “technical details such as their origin estimation, phenotype and health information, photos and identification data, [and] raw data,” among other data points. The hacker added that the Data Breach compromised “13M pieces of data,” and that “[e]ach raw data [file] is around 20-30 MB in size.”



Source: Recorded Future News²²

23. On October 4, 2023, under the heading “23andMe – Genetic Data For Sale,” the hacker posted again, claiming to have “tailored ethnic groupings, individualized data sets, pinpointed origin estimations, haplogroup details, phenotype information, photographs, links to

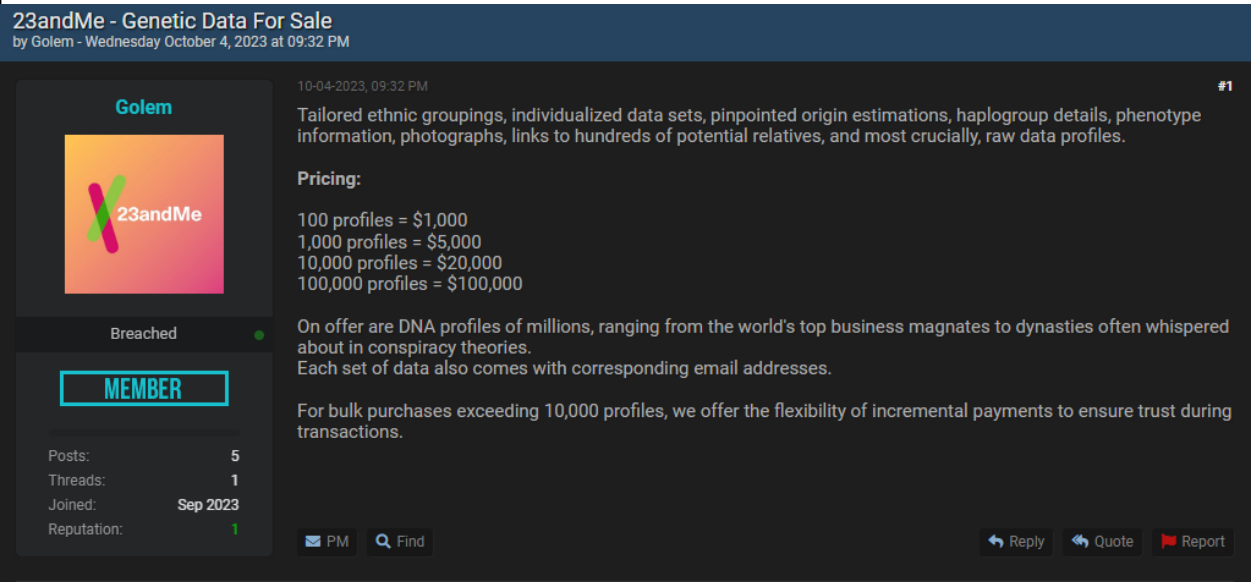
<https://breachforums.is/Thread-DNA-Data-of-Celebrities-1-million-Ashkenazi-REPOST> [<https://webcache.googleusercontent.com/search?q=cache:Tk1as80qBkYJ:https://breachforums.is/Thread-DNA-Data-of-Celebrities-1-million-Ashkenazi-REPOST>]; DNA Data of Celebrities (100,000 Chinese), BreachForums (Oct. 2, 2023), <https://breachforums.is/Thread-DNA-Data-of-Celebrities-100-000-Chinese> [<https://webcache.googleusercontent.com/search?q=cache:BHqAR1agkKoJ:https://breachforums.is/Thread-DNA-Data-of-Celebrities-100-000-Chinese>].

²² Jonathan Greig, *23andMe scraping incident leaked data on 1.3 million users of Ashkenazi and Chinese descent*, RECORDED FUTURE NEWS (Oct. 6, 2023), <https://therecord.media/scraping-incident-genetic-testing-site> [<https://web.archive.org/web/20231006200925/https://therecord.media/scraping-incident-genetic-testing-site>].

hundreds of potential relatives, and most crucially, raw data profiles.”²³ The hacker offered the data for sale in 100, 1,000, 10,000 and 100,000-profile batches.²⁴

23andMe - Genetic Data For Sale
by Golem - Wednesday October 4, 2023 at 09:32 PM

10-04-2023, 09:32 PM #1



Tailored ethnic groupings, individualized data sets, pinpointed origin estimations, haplogroup details, phenotype information, photographs, links to hundreds of potential relatives, and most crucially, raw data profiles.

Pricing:

100 profiles =	\$1,000
1,000 profiles =	\$5,000
10,000 profiles =	\$20,000
100,000 profiles =	\$100,000

On offer are DNA profiles of millions, ranging from the world's top business magnates to dynasties often whispered about in conspiracy theories. Each set of data also comes with corresponding email addresses.

For bulk purchases exceeding 10,000 profiles, we offer the flexibility of incremental payments to ensure trust during transactions.

Posts: 5
Threads: 1
Joined: Sep 2023
Reputation: 1

PM Find Reply Quote Report

Source: Bleeping Computer²⁵

24. On October 6, 2023, 23andMe confirmed that PII and PGI had been compromised in the Data Breach, stating in a post on its website:

We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorization.

[. . .]

We believe that the threat actor may have . . . accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles, to the extent a user opted into that service.²⁶

²³ AJ Vicens, *DNA testing service 23andMe investigating theft of user data*, CYBERSCOOP (Oct. 5, 2023), <https://cyberscoop.com/23andme-user-data-theft/>.

²⁴ *Id.*

²⁵ Toulas, *supra* n.21.

²⁶ Addressing Data Security Concerns (Oct. 6, 2023), <https://blog.23andme.com/articles/addressing-data-security-concerns> [<https://web.archive.org/web/20231007110808/https://blog.23andme.com/articles/addressing-data-security-concerns>].

1 25. On October 9, 2023, 23andMe updated its post to state:

2 We are reaching out to our customers to provide an update on the
3 investigation and to encourage them to take additional actions to
4 keep their account and password secure. Out of caution, we are
5 requiring that all customers reset their passwords and are
6 encouraging the use of multi-factor authentication (MFA).

7 If we learn that a customer's data has been accessed without their
8 authorization, we will notify them directly with more information.²⁷

9 26. 23andMe identifies the specific data elements potentially available through the
10 DNA Relatives profiles, including display name, recent login activity, genetic gender, predicted
11 relationship and percentage of DNA shared with potential family members, ancestry composition,
12 maternal and paternal haplogroups, Neanderthal ancestry results, matching DNA segments, birth
13 location, current location, profile picture, birth year, family trees, and any other family information
14 entrusted to 23andMe.²⁸

15 27. 23andMe blamed its customers for the breach, claiming that it believed "threat
16 actors were able to access certain accounts" where "usernames and passwords that were used on
17 23andMe.com were the same as those used on other websites that have been previously hacked."²⁹

18 28. 23andMe's response was merely "encouraging" users to enable multi-factor
19 authentication.

20 29. Multi-factor authentication works by requiring users to provide more than a mere
21 password to login to a website; users must instead provide a second factor of authentication,
22 usually a code generated by an application or sent via text, to login, ensuring that the individual
23 presenting the password is the same individual with access to the device presenting the
24 authentication code.

25 ²⁷ *Id.*

26 ²⁸ DNA Relatives Privacy and Display Settings, [https://customercare.23andme.com/hc/en-](https://customercare.23andme.com/hc/en-us/articles/18262768896023)
27 us/articles/18262768896023 [https://web.archive.org/web/20231015073225/
28 <https://customercare.23andme.com/hc/en-us/articles/18262768896023>].

²⁹ Addressing Data Security Concerns, *supra* n.26.

30. If 23andMe's belief as to the cause of the Data Breach were correct, requiring users to enable multi-factor authentication could have prevented the Data Breach.

31. Requiring users to enable multi-factor authentication is considered by security researchers and industry professionals to be "[b]asic security hygiene" that "can protect against 98% of attacks."³⁰ That's why, according to Microsoft, "almost all online services - banks, social media, shopping" use multi-factor authentication to secure accounts.³¹ Similarly, according to Google: "One of the best ways to protect your account from a breached or bad password is by having a second form of verification in place – another way for your account to confirm it is really you logging in."³² That's why in 2021, Google began "automatically enrolling" users in multi-factor authentication.³³

32. To this day, 23andMe has not required its users to enroll in multi-factor authentication.

C. Plaintiff's PII and PGI Was Compromised in the Data Breach

33. Plaintiff paid approximately \$100 to purchase a 23andMe testing kit and provided her PII and PGI to 23andMe in approximately 2015.

34. On October 12, 2023, 23andMe provided notice of the Data Breach to Plaintiff and stated: "If we learn that your data has been accessed without your authorization, we will contact you separately with more information."

35. On October 24, 2023, 23andMe provided a supplemental notice to Plaintiff that stated in relevant part: "After further review, we have identified your DNA Relatives profile as

³⁰ Andrea Fisher, *Is MFA the Vegetable of Cybersecurity?*, DARK READING (Dec. 1, 2022), <https://www.darkreading.com/microsoft/is-mfa-the-vegetable-of-cybersecurity>.

³¹ *What is: Multifactor Authentication*, <https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661> ("Compromised passwords are one of the most common ways that bad guys can get at your data, your identity, or your money. Using multifactor authentication is one of the easiest ways to make it a lot harder for them.").

³² Mark Risher, *A simpler and safer future — without passwords*, GOOGLE (May 6, 2021), <https://blog.google/technology/safety-security/a-simpler-and-safer-future-without-passwords/>.

³³ *Id.*

one that was impacted in this incident. Specifically, there was unauthorized access to one or more 23andMe accounts that were connected to you through DNA Relatives. As a result, the DNA Relatives profile information you provided in this feature was exposed to the threat actor.”

36. Plaintiff would not have purchased a 23andMe testing kit or provided her PII and PGI to 23andMe if she had known that 23andMe had failed to implement and maintain reasonable security measures adequate to secure her PII and PGI.

37. As a direct and proximate result of 23andMe’s conduct, Plaintiff has lost the ability to control the use and dissemination of her PII and PGI.

D. 23andMe Specifically Knew of the Risk of the Data Breach

38. The risk of the Data Breach was eminently foreseeable to 23andMe. In its Form 10-K statement, 23andMe specifically acknowledged and warned of the risk of a data breach that could compromise PII and PGI:

Increased global IT security threats and more sophisticated and targeted computer crime pose a risk to the security of our systems and networks and the confidentiality, availability, and integrity of our data. There have been several recent, highly publicized cases in which organizations of various types and sizes have reported the unauthorized disclosure of customer or other confidential information, as well as cyberattacks involving the dissemination, theft, and destruction of corporate information, intellectual property, cash, or other valuable assets. There have also been several highly publicized cases in which hackers have requested “ransom” payments in exchange for not disclosing customer or other confidential information or for not disabling the target company’s computer or other systems. A security breach or privacy violation that leads to disclosure or unauthorized use or modification of, or that prevents access to or otherwise impacts the confidentiality, security, or integrity of, sensitive, confidential, or proprietary information we or our third-party service providers maintain or otherwise process, could compel us to comply with breach notification laws, and cause us to incur significant costs for remediation, fines, penalties, notification to individuals and governmental authorities, implementation of measures intended to repair or replace systems or technology, and to prevent future occurrences, potential increases in insurance premiums, and forensic security audits or investigations. Additionally, a security compromise of our information systems or of those of businesses with whom we interact that results in confidential information being accessed by unauthorized or improper persons could harm our reputation and expose us to customer and patient attrition, and

claims brought by our customers, patients, or others for breaching contractual confidentiality and security provisions or data protection laws. Monetary damages imposed on us could be significant and not covered by our liability insurance.³⁴

39. 23andMe bluntly acknowledged that its customers, including Plaintiff and Class members, considered it material that 23andMe had implemented and maintained reasonable data security measures adequate to protect PII and PGI, stating that “[e]ven the *perception* that the privacy of personal information is not satisfactorily protected or does not meet regulatory requirements could inhibit sales of our solutions. . . .” [Emphasis added.]³⁵

40. The risks of data breaches has long been well-known. In 2015, IBM’s CEO warned: “Cyber crime is the greatest threat to every company in the world.”³⁶ The number of U.S. data breaches surpassed 1,000 in 2016, a 40% increase in the number of data breaches from the previous year.³⁷ In 2017, a new record high of 1,579 breaches were reported representing a 44.7% increase.³⁸ That upward trend continues.

41. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.³⁹

³⁴ Form 10-K, *supra* n.7.

³⁵ *Id.*

³⁶ Sofia Said Birch, *IBM’s CEO on hackers: “Cyber crime is the greatest threat to every company in the world,”* IBM NORDIC BLOG (Nov. 15, 2015), <https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/>.

³⁷ *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, CISION PR NEWSWIRE (Jan. 19, 2017), <https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html>.

³⁸ *2017 Annual Data Breach Year-End Review*, IDENTITY THEFT RES. CTR., <https://www.idtheftcenter.org/wp-content/uploads/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf>.

³⁹ *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf.

42. A robust black market exists in which criminals openly post stolen PII, PGI, and related information on the dark web.

43. PII and PGI have tremendous value. According to the FTC, if hackers get access to personally identifiable information, they will use it.⁴⁰ While credit card information and associated PII can sell for as little as \$1-\$2 on the black market, health information alone can sell for as much as \$363.⁴¹ Because of its immutability, PGI is worth even more.

44. The Federal Trade Commission Act (“FTCA”) (15 U.S.C. §45) prohibited 23andMe from engaging in “unfair or deceptive acts or practices in or affecting commerce.” According to the FTC, a company’s failure to implement or maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTCA.

45. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁴²

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.⁴³ The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

⁴⁰ Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM’N (May 24, 2017), <https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

⁴¹ See *Data Breaches: In the Healthcare Sector*, CTR. FOR INTERNET SEC., <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/> (last visited Nov. 7, 2023).

⁴² *Start With Security: A Guide for Business*, FED. TRADE COMM’N, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

⁴³ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION: <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last visited Nov. 7, 2023).

1 understand their network's vulnerabilities; and implement policies to correct any security
2 problems.

3 47. The FTC further recommends that companies not maintain PII or PGI longer than
4 is needed; limit access to private data; require complex passwords to be used on networks; use
5 industry-tested methods for security; and monitor for suspicious activity on the network.⁴⁴

6 48. The FTC has brought enforcement actions against businesses for failing to
7 adequately and reasonably protect customer data, treating the failure to employ reasonable and
8 appropriate measures to protect against unauthorized access to confidential consumer data as an
9 unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. §45. Orders resulting from
10 these actions further clarify the measures businesses must take to meet their data security
11 obligations.

12 49. 23andMe failed to implement or maintain reasonable data security measures
13 adequate to protect PII and PGI. 23andMe's failure constitutes an unfair act or practice prohibited
14 by Section 5 of the FTCA, 15 U.S.C. §45.

15 **CLASS ACTION ALLEGATIONS**

16 50. Plaintiff brings this class action on behalf of herself and on behalf of all others
17 similarly situated pursuant to California Code of Civil Procedure § 382.

18 51. Plaintiff seeks certification of a Class currently defined⁴⁵ as follows:

19 All citizens of the State of California whose PII and PGI were
20 compromised in the data breach of 23andMe's systems.

21 52. Excluded from the Class are: Defendants and its subsidiaries and affiliates; all
22 employees of Defendants; all persons who make a timely election to be excluded from the Class;
23 and the judge to whom this case is assigned, including his/her immediate family and court staff.

24 53. **Numerosity:** The Class is so numerous that joinder of all members is impracticable.
25 The hacker associated with the Data Breach claims to have data associated with millions of
26

27 ^{44.} *Id.*

28 ⁴⁵ Plaintiff reserve the right to amend the definition of the proposed Class.

1 individuals whose PII and PGI was compromised. In connection with providing notice of the Data
 2 Breach, 23andMe has confirmed that it can identify individuals whose data was accessed without
 3 their authorization.

4 54. **Commonality and Predominance:** This action involves common questions of law
 5 and fact, which predominate over any questions affecting individual Class members, including,
 6 without limitation:

7 A. whether 23andMe engaged in the misconduct alleged;

8 B. whether 23andMe implemented and maintained data security measures that
 9 were inadequate to protect Plaintiff and Class members' PII and PGI;

10 C. whether 23andMe owed a duty to Plaintiff and Class members and whether
 11 23andMe breached that duty;

12 D. whether 23andMe engaged in unfair or unlawful acts and practices;

13 E. whether Plaintiff and Class members were injured and suffered damages as a
 14 result of 23andMe's conduct; and

15 F. whether Plaintiff and Class members are entitled to relief and the measure of
 16 such relief.

17 55. **Typicality:** Plaintiff had her PII and PGI compromised in the Data Breach.
 18 Plaintiff's claims are typical of the other Class members' claims because, among other things, all
 19 Class members were comparably injured through Defendant's conduct and Plaintiff and each Class
 20 member would assert claims based on the same legal theories.

21 56. **Adequacy:** Plaintiff is an adequate Class representative because she is a member
 22 of the Class she seeks to represent and her interests do not conflict with the interests of the other
 23 members of the Class that she seeks to represent. Plaintiff is committed to pursuing this matter
 24 for the Class with the Class's collective best interests in mind. Plaintiff has retained counsel
 25 competent and experienced in complex class action litigation of this type, and Plaintiff intends to
 26 prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the
 27 Class's interests.
 28

57. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against 23andMe, so it would be impracticable for members of the Class to individually seek redress for 23andMe's conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

58. **Injunctive and Declaratory Relief:** 23andMe, through its uniform conduct, acted or refused to act on grounds generally applicable to each Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Unless a Class-wide injunction is issued, Plaintiff and Class members remain at risk that Defendant will continue to fail to properly secure their PII and PGI, potentially resulting in another data breach.

FIRST CLAIM FOR RELIEF
Negligence

59. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

60. Plaintiff brings this claim on behalf of herself and the Class.

61. 23andMe required Plaintiff and members of the Class to submit PII and PGI to use 23andMe's services.

62. 23andMe knew or should have known of the risks inherent in collecting and storing Plaintiff and Class members' PII and PGI.

63. 23andMe owed a duty of care to Plaintiff and Class members who entrusted their PII and PGI to 23andMe.

64. A special relationship exists between 23andMe and Plaintiff and members of the Class because Plaintiff and members of the Class entrusted their PII and PGI to 23andMe.

65. 23andMe breached its duty of care to Plaintiff and Class members by failing to implement or maintain reasonable security measures adequate to protect Plaintiff and Class members' PII and PGI.

66. As a direct and proximate result of 23andMe's negligent conduct, Plaintiff and members of the Class have been injured.

67. The injuries suffered by Plaintiff and members of the Class were the reasonably foreseeable result of 23andMe's breach of its duty of care to Plaintiff and Class members.

68. Plaintiff and members of the Class are entitled to damages and other relief as this Court considers necessary and proper.

SECOND CLAIM FOR RELIEF

Negligence Per Se

69. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

70. Plaintiff brings this claim on behalf of herself and the Class.

71. 23andMe required Plaintiff and members of the Class to submit PII and PGI to use 23andMe's services.

72. 23andMe knew or should have known of the risks inherent in collecting and storing Plaintiff and Class members' PII and PGI.

73. 23andMe owed a duty of care to Plaintiff and Class members who entrusted their PII and PGI to 23andMe.

74. Pursuant to the FTC Act, 15 U.S.C. §45(a)(1), California's Consumer Privacy Act, Cal. Civ. Code §1798.100 (Deering) Cal. Civ. Code §1798.150, and California's Genetic Information Privacy Act, Cal. Civ. Code §56.18 (Deering), 23andMe had a duty to implement and maintain reasonable security measures adequate to protect Plaintiff's and Class members' PII and PGI.

75. 23andMe breached its duty of care to Plaintiff and Class members by failing to implement or maintain reasonable security measures adequate to protect Plaintiff and Class members' PII and PGI in violation of the FTC Act, California's Consumer Privacy Act, and California's Genetic Information Privacy Act.

76. As a direct and proximate result of 23andMe's negligent conduct, Plaintiff and members of the Class have been injured.

77. The injuries suffered by Plaintiff and members of the Class were the reasonably foreseeable result of 23andMe's breach of its duty of care to Plaintiff and Class members.

78. Plaintiff and members of the Class are entitled to damages and other relief as this Court considers necessary and proper.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract

79. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

80. Plaintiff brings this claim on behalf of herself and the Class.

81. 23andMe required Plaintiff and members of the Class to pay 23andMe and to submit PII and PGI to use 23andMe's services.

82. 23andMe impliedly agreed to implement and maintain reasonable data security measures that complied with industry standards and was adequate to protect PII and PGI in exchange for receiving Plaintiff and Class members' PII, PGI, and payments.

83. Plaintiff and members of the Class paid 23andMe and submitted their PII and PGI to 23andMe.

84. Plaintiff and members of the Class would not have paid 23andMe or submitted their PII and PGI to 23andMe unless 23andMe agreed to implement and maintain reasonable data security measures that complied with industry standards and was adequate to protect PII and PGI.

85. 23andMe breached its agreements with Plaintiff and members of the Class by implementing and maintaining unreasonable data security measures that were inadequate to protect PII and PGI or prevent the Data Breach.

1 86. As a direct and proximate result of 23andMe's conduct, Plaintiff and members of
2 the Class have been damaged.

3 87. Plaintiff and members of the Class are entitled to damages and other relief as this
4 Court considers necessary and proper.

5 **FOURTH CLAIM FOR RELIEF**
6 **Invasion Of Privacy**

7 88. Plaintiff incorporates and realleges each and every allegation contained above as if
8 fully set forth herein.

9 89. Plaintiff brings this claim on behalf of herself and the Class.

10 90. 23andMe intruded on Plaintiff and Class members' seclusion or solitude, without
11 consent, by causing an unreasonable, substantial, and serious interference with the privacy of
12 Plaintiff and Class members' PII and PGI.

13 91. Plaintiff and members of the Class have an objective, reasonable expectation of
14 privacy in their PII and PGI.

15 92. Plaintiff and members of the Class did not consent to, authorize, or know about
16 23andMe's interference with the privacy of their PII and PGI.

17 93. 23andMe's conduct is highly objectionable to a reasonable person and constitutes
18 an egregious breach of the social norms underlying the right to privacy.

19 94. 23andMe's conduct was intentional insofar as the risk of a data breach and the
20 purported vector of the Data Breach was well-known within the industry and 23andMe
21 intentionally failed to implement or maintain reasonable security measures adequate to protect
22 Plaintiff and members of the Class's PII and PGI.

23 95. 23andMe's conduct has harmed Plaintiff and members of the Class by causing them
24 mental anguish and suffering arising from their loss of privacy and confidentiality of their PII and
25 PGI.

26 96. 23andMe's conduct has deprived Plaintiff and members of the Class of their right
27 to control the use and dissemination of their PII and PGI.
28

1 97. Plaintiff and members of the Class are entitled to damages and other relief as this
2 Court considers necessary and proper.

3 **FIFTH CLAIM FOR RELIEF**
4 **Conversion**

5 98. Plaintiff incorporates and realleges each and every allegation contained above as if
6 fully set forth herein.

7 99. Plaintiff brings this claim on behalf of herself and the Class.

8 100. Plaintiff and members of the Class have an interest in maintaining their right to
9 control the use and dissemination of their PII and PGI.

10 101. 23andMe has exercised dominion over Plaintiff and Class members' PII and PGI
11 by disclosing it without their permission.

12 102. As a direct and proximate result of 23andMe's conduct, Plaintiff and members of
13 the Class have lost the exclusive right to control the use and dissemination of their PII and PGI.

14 103. Plaintiff and members of the Class are entitled to damages and other relief as this
15 Court considers necessary and proper.

16 **SIXTH CLAIM FOR RELIEF**
17 **Violation of The California Unfair Competition Law,**
18 **Cal. Bus. & Prof. Code §17200 Based On "Unfair" and/or "Unlawful" Acts and Practices**

19 104. Plaintiff incorporates and realleges each and every allegation contained above as if
20 fully set forth herein.

21 105. Plaintiff brings this claim on behalf of herself and the Class pursuant to the
22 California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200.

23 106. Plaintiff and 23andMe are "persons" within the meaning of Cal. Bus. & Prof. Code
24 §17201.

25 107. The UCL prohibits unfair competition, which includes an "unlawful, unfair or
26 fraudulent" act or practice. Cal. Bus. & Prof. Code §17200.

1 108. Under the UCL, any business act or practice that is unethical, oppressive,
2 unscrupulous, and/or substantially injurious to consumers, or that violates a legislatively declared
3 policy, constitutes an unfair business act or practice.

4 109. The violation of any law constitutes an unlawful business practice under the UCL.

5 110. 23andMe engaged in unfair and unlawful business practices prohibited by the UCL
6 by implementing and maintaining unreasonable data security measures that were inadequate to
7 protect PII and PGI or prevent the Data Breach. These unfair and unlawful practices occurred in
8 connection with 23andMe's trade or business.

9 111. 23andMe's affirmative acts in implementing and maintaining unreasonable data
10 security measures were unfair within the meaning of the UCL, because they constituted immoral,
11 unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers, and
12 provided no benefit to consumers.

13 112. 23andMe's implementation of inadequate and unreasonable data security measures
14 also was unfair within the meaning of the UCL, because its conduct undermined California public
15 policy that businesses protect personal information as reflected in Article I, Section 1 of the
16 California Constitution (enacted because of private sector data processing activity and stating that
17 all people have an inalienable right to privacy) and in statutes such as the Online Privacy Protection
18 Act, Cal. Bus. & Prof. Code §22578 (explaining that the Legislature's intent was to have a uniform
19 policy statewide regarding privacy policies on the Internet); the Information Practices Act, Cal.
20 Civ. Code §1798.1 ("The Legislature declares that. . . all individuals have a right of privacy in
21 information pertaining to them . . . The increasing use of computers. . . has greatly magnified the
22 potential risk to individual privacy that can occur from the maintenance of personal information.");
23 *id.*, §1798.81.5(a)(1); and the FTC Act, 15 U.S.C. §45(a)(1), which prohibits unfair trade practices.

24 113. 23andMe's violations of the California Customer Records Act, Cal. Civ. Code
25 §1798.81.5(b) (the "California Customer Records Act"), moreover, constitute unlawful acts or
26 practices under the UCL. The California Customer Records Act requires a "business that owns,
27 licenses, or maintains personal information about a California resident" to "implement and
28 maintain reasonable security procedures and practices appropriate to the nature of the information"

1 and “to protect the personal information from unauthorized access, destruction, use, modification,
2 or disclosure.” 23andMe failed to implement and maintain such reasonable security procedures
3 and practices before and at the time of the Data Breach. As a result, 23andMe violated the
4 California Customer Records Act, *id.*

5 114. 23andMe’s violations of the FTC Act, 15 U.S.C. §45(a)(1) and California’s Genetic
6 Information Privacy Act, Cal. Civ. Code §56.18 (“GIPA”), also constitute unlawful acts or
7 practices under the UCL. The GIPA requires a “direct-to-consumer genetic testing company” to
8 “[i]mplement and maintain reasonable security procedures and practices to protect a consumer’s
9 genetic data against unauthorized access, destruction, use, modification, or disclosure.”
10 §56.181(d)(1). 23andMe violated §56.181(d)(1) by failing to implement and maintain reasonable
11 security procedures and practices to protect Plaintiff and the Class members’ PGI against
12 unauthorized access, use, and disclosure.

13 115. Plaintiff and the Class reasonably expected 23andMe to implement and maintain
14 reasonable data security measures that complied with industry standards and could prevent the
15 Data Breach and protect PII and PGI.

16 116. Plaintiff and members of the Class had no knowledge and could not have
17 reasonably known that 23andMe implemented and maintained unreasonable data security
18 measures. Because 23andMe was solely responsible for implementing and maintaining reasonable
19 data security measures to protect PII and PGI, neither Plaintiff nor members of the Class could
20 have avoided the injuries they sustained.

21 117. There were reasonably available alternatives to further 23andMe’s legitimate
22 business interests, other than its conduct responsible for the Data Breach.

23 118. 23andMe’s conduct has deprived Plaintiff and members of the Class of their right
24 to control the use and dissemination of their PII and PGI.

25 119. 23andMe willfully engaged in the unfair and unlawful acts and practices described
26 above and knew or should have known that those acts and practices were unfair and unlawful in
27 violation of the UCL.

28

120. As a direct and proximate result of 23andMe's unfair and unlawful practices and violation of UCL, Plaintiff and the Class have suffered injury in fact and have lost money and property. Plaintiff and members of the Class lost money as a result of 23andMe's violation of the GIPA because they paid for a service with reasonable data security measures adequate to protect PII and PGI and prevent the Data Breach but received a service with unreasonable data security measures inadequate to protect PII and PGI or prevent the Data Breach. Plaintiff and members of the Class lost property as a result of 23andMe's violation of the GIPA because they no longer have the exclusive right to control the use and dissemination of their PII and PGI.

121. Plaintiff is entitled to restitution and other relief as this Court considers necessary and proper.

SEVENTH CLAIM FOR RELIEF
Violation of The California Consumer Privacy Act

122. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

123. Plaintiff brings this claim on behalf of herself and the Class pursuant to the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §1798.100 1798.150.

124. PII and PGI constitute "personal information" within the meaning of *id.*, §1798.81.5(d)(1)(A).

125. The PII and PGI compromised in the Data Breach was nonencrypted and nonredacted.

126. Plaintiff and Class members' PII and PGI was disclosed as a result of 23andMe's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII and PGI of Plaintiff and Class members.

127. 23andMe's misconduct was egregious and serious and has resulted in the violation of the CCPA as to millions of Class members. 23andMe's conduct was intentional insofar as the risk of a data breach and the purported vector of the Data Breach were well-known within the industry and 23andMe intentionally failed to implement or maintain reasonable security measures

adequate to protect Plaintiff and members of the Class's PII and PGI. 23andMe has substantial assets, liabilities, and net worth.

128. On November 2, 2023, Plaintiff sent 23andMe pre-suit notice demand letters, pursuant to *id.*, §1798.150.

129. Plaintiff and members of the Class are entitled to damages and other relief as this Court considers necessary and proper.

EIGHTH CLAIM FOR RELIEF
Unjust Enrichment

130. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

131. Plaintiff brings this claim on behalf of herself and the Class.

132. Plaintiff and members of the Class conferred a benefit on 23andMe in the form of payments made for the purchase of genetic testing kits and in the form of PII and PGI that Plaintiff and Class members provided to 23andMe.

133. 23andMe appreciated or had knowledge of the benefits conferred upon it by Plaintiff and members of the Class. 23andMe continues to store Plaintiff's and Class members' PII and PGI and to derive benefits from such PII and PGI by using it to drive insights that 23andMe can monetize.

134. Under principles of equity and good conscience, 23andMe should not be permitted to retain the benefits of Plaintiff and members of the Class. 23andMe could have but chose not to implement or maintain reasonable data security measures adequate to protect PII and PGI as required by law and industry standards and compromised Plaintiff and Class members' exclusive right to control the use and dissemination of their PII and PGI.

135. Neither Plaintiff nor Class members have an adequate remedy at law. Monetary damages alone are incapable of restoring to Plaintiff or Class members the exclusive right to control the use and dissemination of their PII and PGI, which has been compromised as a direct and proximate result of the Data Breach.

PRAYER FOR RELIEF

136. WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendant and in favor of Plaintiff and the Class and award the following relief:

A. that this action be certified as a class action, pursuant to California Code of Civil Procedure §382, declaring Plaintiff as a representative of the Class and Plaintiff's counsel as counsel for the Class;

B. monetary damages;

C. injunctive relief;

D. reasonable attorneys' fees and expenses, including those related to experts and consultants;

E. costs;

F. pre- and post-judgment interest; and

G. such other relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, demands a trial by jury for all issues so triable.

Dated: December 4, 2023

LEXINGTON LAW GROUP



Mark N. Todzo (Bar No. 168389)
Patrick R. Carey (Bar No. 308623)
Meredyth L. Merrow (Bar No. 328337)
503 Divisadero Street
San Francisco, CA 94117

1 Telephone: (415) 913-7800
2 Facsimile: (415) 759-4112
3 mtodzo@lexlawgroup.com

4 Joseph P. Guglielmo (*pro hac vice* forthcoming)
5 Carey Alexander (*pro hac vice* forthcoming)
6 **SCOTT+SCOTT ATTORNEYS AT LAW LLP**
7 The Helmsley Building
8 230 Park Avenue, 17th Floor
9 New York, NY 10169-1820
10 Telephone: (212) 223-6444
11 Facsimile: (212) 223-6334
12 jguglielmo@scott-scott.com
13 calexander@scott-scott.com

14 *Attorneys for Plaintiff*
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Exhibit C

Potter Handy, LLP
Mark Potter, Esq., SBN 166317
Barry Walker, Esq., SBN 195947
Jim Treglio, Esq., SBN 228077
Christina Carson, Esq. SBN 280048
Tehniat Zaman, Esq. SBN 321557
Mail: 100 Pine St., Ste. 1250
San Francisco, CA 94111
(415) 534-1911; (888) 422-5191 fax
23andMeIL@potterhandy.com
Attorneys for Plaintiffs

SUPERIOR COURT OF CALIFORNIA
SANTA CLARA COUNTY

**TRISHA WILKUS; RYAN FOWLER;
ARTURO GONZALEZ; SARAH
SCHULTZ; CASSANDRA
SALGADO; MELANIE DIMUZIO;
DARLENE EBY; SANDY
LANDVICK; DALIA RAMAHI;
PATTY ZINK; KATHARINA
RYASATI; STEVE TEMKIN; AND
NICOLE CASSIDY,**

Plaintiff,

v.

23ANDME, INC.,

Defendant.

Case No.

**COMPLAINT FOR CIVIL
DAMAGES AND INJUNCTIVE
RELIEF**

- 1. Illinois Genetic Information
Privacy Act**
- 2. Negligence**
- 3. Breach Of Actual and Implied
Contract**
- 4. Invasion Of Privacy –
Intrusion Upon Seclusion**
- 5. Unjust Enrichment**

JURY TRIAL DEMANDED

COMPLAINT

Plaintiffs Trisha Wilkus; Ryan Fowler; Arturo Gonzalez; Sarah Schultz;
Cassandra Salgado; Melanie DiMuzio; Darlene Eby; Sandy Landvick; Dalia Ramahi;
Patty Zink; Katharina Ryasati; Steve Temkin; and Nicole Cassidy, (collectively

1 “Plaintiffs”) allege against Defendant 23andMe, Inc. (“23andMe” or “Defendant”) as
2 follows:

3 **SUMMARY:**

- 4
- 5 1. Defendant is a genomic and biotechnology company that looks at an individual’s
6 genome for the purpose of creating unique, personalized genetic reports on
7 ancestral origins, personal genetic health risks, chances of passing on carrier
8 conditions, and pharmacogenetics.¹
 - 9 2. To take advantage of Defendant’s services, customers had to provide sensitive
10 personal, genetic, and biological information. To gain the trust of potential
11 customers Defendant expressly advertised the importance of security as “Privacy is
12 in our DNA”.
 - 13 3. On or about October 6, 2023, Defendant announced, via their website, that
14 unauthorized threat actors had accessed 23andMe accounts and compiled customer
15 profile information (the “Data Breach”).²
 - 16 4. The Data Breach contained millions of individuals’ private identifying information
17 (hereinafter “PII”), including, but not limited to: names, sex, date of birth,
18 usernames, genetic ancestry, profile photos, geographical locations, living
19 biological relatives, and data about individuals’ ethnicity.
 - 20 5. Plaintiffs are customers of 23andMe that were victims of the Data Breach. Due to
21 the Data Breach, Plaintiffs’ PII was released, stolen, and offered for sale on the dark
22 web.
 - 23 6. Defendant had a non-delegable duty and responsibility to implement and maintain
24 reasonable security measures to secure, safeguard, and protect the private
25 information that it collected, stored, and maintained for Plaintiffs.
 - 26 7. Defendant disregarded the rights of Plaintiffs by intentionally, willfully, recklessly,
27 or negligently failing to implement adequate and reasonable measures to ensure that

28 ¹ <https://www.23andme.com/#> (last visited January 9, 2024).

² <https://blog.23andme.com/articles/addressing-data-security-concerns>

1 Plaintiffs' PII was safeguarded, failing to take all available steps to prevent
2 unauthorized disclosure of data, and failing to follow applicable, and appropriate
3 protocols, policies, and procedures regarding the encryption of data. The Data
4 Breach was a direct result of Defendant's failure to implement adequate and
5 reasonable cyber-security procedures and protocols necessary to protect victims'
6 PII.

7 8. As a result of Defendant's failure to implement adequate data security measures,
8 Plaintiffs have suffered actual harm in the disclosure of their PII to unknown and
9 unauthorized third parties. Plaintiffs have suffered injury and ascertainable losses in
10 the form of the present and imminent threat of fraud and identity theft, loss of the
11 benefit of their bargain, out-of-pocket expenses, loss of value of their time
12 reasonably incurred to remedy or mitigate the effects of the attack, and the loss of,
13 and diminution in, value of their PII. Plaintiffs also remain vulnerable to future
14 cyberattacks and thefts from the data in Defendant's possession.

15 9. As such, Plaintiffs assert claims for Illinois Genetic Information Privacy Act
16 (GIPA), 410 ILCS 513 *et seq.*; negligence, breach of implied contract, invasion of
17 privacy, and unjust enrichment.

18 **JURISDICTION AND VENUE:**
19

20 10. This Court has subject matter jurisdiction over this action pursuant to Article VI,
21 section 10 of the California Constitution and Code of Civil Procedure section
22 410.10

23 11. This Court has personal jurisdiction over Defendant because it is headquartered in
24 the State of California, county of Santa Clara, and purposefully avails itself of the
25 laws, protections, and advantages of this State.

26 12. Venue is proper in this Court because Defendant conducts business in this County
27 and reaped substantial profits from customers in this County. In addition, in its own
28 Terms of Service, Defendant has agreed "...to submit to the exclusive jurisdiction

of any state or federal court located in Santa Clara County, California (except for small claims court actions which may be brought in the county where you reside), and waive any jurisdictional, venue, or inconvenient forum objections to such courts.” Finally, a substantial part of the acts and conduct charged herein occurred in this County.

PARTIES:

13. Plaintiffs are residents of Illinois who provided 23andMe with a DNA sample for analysis and whose private identifying information was compromised by the Data Breach.
14. Defendant 23andMe, Inc. is a biotechnology company headquartered in California that collects and analyzes an individual’s genome for the purpose of creating personalized genetic reports directly to consumers.

FACTUAL ALLEGATIONS:

Defendant collected and stored Plaintiffs’ PII

15. Defendant collects PII from their customers in the course of doing business.
16. As a condition of receiving Defendant’s services, Plaintiffs were required to entrust Defendant with highly sensitive genetic information, information derived from genetic testing, health information, ancestral origin, and other confidential and sensitive PII. 23andMe then stores that information in its platform.
17. According to the Privacy Statement on 23andMe’s website, the company collects the following categories of customer information:
 - a) Registration Information, including name, user ID, password, date of birth, billing address, shipping address, payment information, account authentication information, and contact information (such as email address and phone number).
 - b) Genetic information, including “[i]nformation regarding your genotype (e.g., the

- 1 As, Ts, Cs, and Gs at particular locations in your DNA)” and “the 23andMe
2 genetic data and reports provided to you as part of our Services.”
- 3 c) Sample Information, including “[i]nformation regarding any sample, such as a
4 saliva sample, that you submit for processing to be analyzed to provide you with
5 Genetic Information, laboratory values or other data provided through our
6 Services.”
- 7 d) Self-Reported Information, including “gender, disease conditions, health related
8 information, traits, ethnicity, family history, or anything else you want to provide
9 to us within our Service(s).”
- 10 e) User Content, including “[i]nformation, data, text, software, music, audio,
11 photographs, graphics, video, messages, or other materials, other than Genetic
12 Information and Self-Reported Information, generated by users of 23andMe
13 Services and transmitted, whether publicly or privately, to or through 23andMe.
14 For example, User Content includes comments posted on our Blog or messages
15 you send through our Services.”
- 16 f) Web-Behavior Information, including “[i]nformation on how you use our Services
17 or about the way your devices use our Services is collected through log files,
18 cookies, web beacons, and similar technologies (e.g., device information, device
19 identifiers, IP address, browser type, location, domains, page views).”
- 20 g) Biometric Information, including “[c]ertain Self-Reported Information you
21 provide to us or our service providers to verify your identity using biological
22 characteristics.”
- 23 18. As part of its advertising, Defendant promises to maintain the confidentiality of
24 Plaintiffs’ PII to ensure compliance with federal and state laws and regulations, and
25 not to use or disclose Plaintiffs’ PII for non-essential purposes.
- 26 19. Defendant’s Privacy Policy states that it “encrypt[s] all sensitive information and
27 conduct[s] regular assessments to identify security vulnerabilities and threats.”³

28 ³ <https://www.23andme.com/privacy/>

- 1 20. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' PII,
2 Defendant assumed legal and equitable duties and knew or should have known that
3 it was responsible for protecting Plaintiffs' PII from unauthorized disclosure.
- 4 21. Additionally, Defendant had and continues to have obligations created by applicable
5 state law, reasonable industry standards, common law, and its own assurances and
6 representations to keep Plaintiffs' PII confidential and to protect such PII from
7 unauthorized access.
- 8 22. Defendant created the reasonable expectation and mutual understanding with
9 Plaintiffs that it would comply with its obligations to Plaintiffs' information,
10 including the PII, confidential and secure from unauthorized access.
- 11 23. Plaintiffs have the utmost privacy interest in the highly sensitive nature of PII, and
12 would not have been induced to purchase the genetic testing offered by Defendant
13 had Defendant not included privacy assurances within its advertising.
- 14 24. Plaintiffs took reasonable steps to maintain the confidentiality of their PII and relied
15 on Defendant to keep their PII confidential and securely maintained, to use this
16 information for business purposes only, and to make only authorized disclosures of
17 this information.

18
19 ***Data Breach***

- 20 25. On October 6, 2023, Defendant revealed that threat actors were able to access
21 customer accounts and obtain customers' PII without authorization and consent.
- 22 26. Despite the prevalence of public announcements of data breach and data security
23 compromises in recent years, Defendant failed to take sufficient steps to protect
24 Plaintiffs' PII from being compromised.
- 25 27. Upon information and belief, Defendant did not require two-factor authentication to
26 protect Plaintiffs' PII at the time of the Data Breach.
- 27 28. Upon information and belief, Defendant did not adequately monitor, secure, and/or
28 encrypt its servers and Plaintiffs' PII.

1 29. Upon information and belief, Defendant could have prevented the Data Breach.

2 30. Upon information and belief, the cyberattack was expressly designed to gain access
3 to private and confidential data, including Plaintiffs' PII.

4 31. Due to Defendant's inadequate security measures, Plaintiffs now face a present,
5 immediate, and ongoing risk of fraud and identity theft and must deal with that
6 threat indefinitely.

7
8 ***Defendant failed to adequately protect the PII and failed to timely notify Plaintiffs their***
9 ***data had been compromised***

10 32. On November 6, 2023—one month after it disclosed the breach—23andMe
11 announced that it was “requiring all customers use a second step of verification to
12 sign into their account.”

13 33. On information and belief, Defendant did not begin notifying Plaintiffs their
14 specific PII had been compromised until on or after December 1, 2023.

15 34. On information and belief, Defendant continues to fail to take reasonable and
16 adequate measure to notify all impacted customers that their PII has been
17 compromised.

18 35. At all relevant times, Defendant had a duty to exercise reasonable care in obtaining,
19 retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's
20 possession from being compromised, lost, stolen, accessed, and misused by
21 unauthorized persons.

22 36. At all relevant times, Defendant had a duty to properly secure the collected PII,
23 encrypt and maintain such information using industry standard methods, create and
24 implement reasonable data security practices and procedures, train its employees,
25 utilize available technology to defend its systems from invasion, act reasonably to
26 prevent foreseeable harm to Plaintiffs, and to promptly notify Plaintiffs when
27 Defendant became aware that Plaintiffs' PII may have been compromised.

28 37. Defendant touted its security and privacy as part of their advertising. Defendant's

duty to use reasonable security measures arose as a result of the Plaintiffs' reasonable reliance on Defendant to secure their highly sensitive personal data. Plaintiffs surrendered the data to obtain Defendant's services under the express condition that Defendant would keep it private and secure. Accordingly, Defendant also has a duty to safeguard their data, independent of any statute.

38. Defendant owed a duty of care to Plaintiffs because they were foreseeable and probable victims of any inadequate data security practices.

Value of the PII

39. PII are highly valuable for identity thieves and personal information is sold on several underground internet websites for \$40 to \$200⁴ per identity.

40. Identity thieves can use PII, such as that of Plaintiffs to perpetrate a variety of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

41. Criminals can also use stolen PII to extort a financial payment by leveraging sensitive healthcare information, for example a sexually transmitted disease or terminal illness, to extort or coerce the victim.

42. Familial relationships and ethnic background can be used to target certain minority groups with threats or even violence.

43. Data breaches involving medical information are more difficult to detect, and take longer to uncover, than normal identity theft. In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief can use private information "to see a doctor, get prescription drugs, buy medical devices, submit

⁴ Anita George, DIGITAL TRENDS, Your personal data is for sale on the dark web. Here's how much it costs (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

claims with your insurance provider, or get other medical care.”⁵ The FTC also warns that if a thief’s health information is mixed with the victim’s it “could affect the medical care [they are] able to get or the health insurance benefits [they are] able to use.”⁶

44. Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiffs. It knew, or should have known, that PII is sought after and valuable target for thieves and that there was a high likelihood this information would be targeted. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

45. Defendant disregarded the rights of Plaintiffs by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs’ PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and/or extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff prompt and accurate notice of the Data Breach.

46. Plaintiffs have suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have fear, stress, anxiety and increased concerns for the loss of their privacy and PII being in the hands of criminals.

47. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

⁵ See What to Know About Medical Identity Theft, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last visited Oct. 2, 2023).

⁶ *Id.*

1 48. As a result of the Data Breach, Plaintiffs are at risk and will continue to be at
2 increased risk of identity theft and fraud for years to come.

3 49. Plaintiffs have a continuing interest in ensuring that their Private Information, which,
4 upon information and belief, remains backed up in Defendant's possession, is
5 protected and safeguarded from future breaches.

6 ***Defendant Fails to Comply with FTC Guidelines***

7 50. The Federal Trade Commission ("FTC") has promulgated numerous guides for
8 businesses which highlight the importance of implementing reasonable data security
9 practices.

10 51. FTC guidelines note that businesses should protect the personal customer
11 information that they keep; properly dispose of personal information that is no
12 longer needed; encrypt information stored on computer networks; understand their
13 network's vulnerabilities; and implement policies to correct any security problems.

14 52. The guidelines also recommend companies not maintain Private Information longer
15 than is needed for authorization of a transaction; limit access to sensitive data;
16 require complex passwords to be used on networks; use industry-tested methods for
17 security; monitor for suspicious activity on the network; and verify that third-party
18 service providers have implemented reasonable security measures. Further, it
19 recommends businesses use an intrusion detection system to expose a breach as
20 soon as it occurs; monitor all incoming traffic for activity indicating someone is
21 attempting to hack the system; watch for large amounts of data being transmitted
22 from the system; and have a response plan ready in the event of a breach.⁷

23 53. The FTC guidelines also form part of the basis of Defendant's duty in this regard.

24 54. Upon information and belief, Defendant was at all times fully aware of its
25 obligation to protect the PII of its customers, Defendant was also aware of the
26 significant repercussions that would result from its failure to do so. Accordingly,

27 ⁷ Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at
28 https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf
(last visited Oct. 2, 2023).

Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs.

Injuries and Damages:

55. As a result of the Data Breach, Plaintiffs have all sustained actual injuries and damages, including: (i) lost or diminished value of their PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) invasion of privacy; (v) loss of benefit of the bargain; (vi) the continued and certainly increased risk to their PII; and (vii) fear, stress, and anxiety.

56. The information disclosed in this Data Breach is impossible to change. Plaintiffs will have to monitor for identity theft and breaches their entire lives. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Plaintiff. This is a reasonable and necessary cost to monitor to protect Plaintiffs from the risk of identity theft that arose from the Data Breach. This is a future cost that Plaintiffs would not need to bear but for Defendant's failure to safeguard their PII.

CLAIMS FOR RELIEF:

COUNT I: Illinois Genetic Information Privacy Act (On behalf of all Plaintiffs).

57. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this complaint.

58. The Genetic Information Privacy Act (GIPA), 410 Ill. Comp. Stat. Ann. 513 *et seq.*, covers "[c]onfidentiality of genetic information" and provides in relevant part: "Except as otherwise provided in this Act, genetic testing and information derived from genetic testing is confidential and privileged and may be released only to the individual tested and to persons specifically authorized, in writing in accordance

1 with Section 30, by that individual to receive the information.” 410 Ill. Comp. Stat.
2 Ann. 513/15(a).

3 59. GIPA incorporates the definition of “genetic information” from 45 C.F.R. §
4 160.103, which defines the term as “information about” an individual’s “genetic
5 tests,” “[t]he genetic tests of family members of the individual,” “[t]he
6 manifestation of a disease or disorder in family members of such individual,” or
7 “[a]ny request for, or receipt of, genetic services, or participation in clinical research
8 which includes genetic services, by the individual or any family member of the
9 individual.”

10 60. GIPA also incorporates the definition of “genetic test” from 45 C.F.R. § 160.103,
11 which defines the term as “an analysis of human DNA, RNA, chromosomes,
12 proteins, or metabolites, if the analysis detects genotypes, mutations, or
13 chromosomal changes.”

14 61. The test performed by 23andMe qualifies as “genetic testing” under GIPA because
15 it detects, inter alia, genotypes and mutations.

16 62. The information compromised in the breach of 23andMe’s platform included
17 genetic information, genetic testing, and information derived from such
18 information. For example, the origin of Plaintiffs’ ancestors, the list of other
19 23andMe users identified by 23andMe as Plaintiff’s DNA relatives, and the
20 information on the number of DNA segments Plaintiffs shared with those other
21 users were all information about, and derived from, the 23andMe genetic test
22 Plaintiff purchased. Moreover, these results serve as a receipt of genetic services
23 performed by 23andMe for Plaintiff.

24 63. 23andMe negligently and recklessly released Plaintiff and class members’ genetic
25 information, PII, and other confidential and highly sensitive PII by failing to
26 adequately safeguard that information from malicious actors. Considering the
27 number of data breaches and the sensitivity of the information it possessed,
28 23andMe was aware or should have been aware of the need to implement robust

1 security measures to protect such information. It consciously refused to do so.

2 64. By negligently and recklessly releasing Plaintiffs' information (including genetic
3 testing and information derived from genetic testing performed by 23andMe) to
4 unauthorized parties, as alleged above, 23andMe violated GIPA.

5 65. Accordingly, Plaintiffs are entitled to, and seek, damages of "\$2,500 or actual
6 damages, whichever is greater," for each negligent violation, or "\$15,000 or actual
7 damages, whichever is greater," for each intentional or reckless violation, as well as
8 reasonable attorney's fees and costs. 410 Ill. Comp. Stat. Ann. 513/40.

9 66. Plaintiffs are also authorized to obtain injunctive relief to prevent future violations.
10 *Id.*

11 **COUNT II: Negligence** (On behalf of all Plaintiffs).

12 67. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this
13 complaint.

14 68. At all times herein relevant, Defendant owed Plaintiffs a duty of care, *inter alia*, to
15 act with reasonable care to secure and safeguard their PII and to use commercially
16 reasonable methods to do so. Defendant took on this obligation upon accepting and
17 storing the PII of Plaintiffs in its computer systems and on its networks.

18 69. Defendant knew that the PII was private and confidential and should be protected
19 and, thus, Defendant owed a duty of care not to subject Plaintiffs to an unreasonable
20 risk of harm because they were foreseeable and probable victims of any inadequate
21 security practices.

22 70. Defendant knew, or should have known, of the risks inherent in collecting and
23 storing PII, the vulnerabilities of its data security systems, and the importance of
24 adequate security.

25 71. Defendant knew, or should have known, that its data systems and networks did not
26 adequately safeguard Plaintiffs' PII.

27 72. Only Defendant was in the position to ensure that its systems and protocols were
28

1 sufficient to protect the PII that Plaintiffs had entrusted to it.

2 73. Because Defendant knew that a breach of its systems could damage thousands of
3 individuals, including Plaintiffs, Defendant had a duty to adequately protect its data
4 systems and the PII contained therein.

5 74. Plaintiffs' willingness to entrust Defendant with their PII was predicated on the
6 understanding that Defendant would take adequate security precautions.

7 75. Moreover, only Defendant had the ability to protect its systems and the PII stored
8 on them from attack.

9 76. Defendant also had independent duties under state laws that required Defendant to
10 reasonably safeguard Plaintiffs' PII and promptly notify them about the Data
11 Breach. These "independent duties" are untethered to any contract between
12 Defendant and Plaintiffs.

13 77. Defendant breached its general duty of care to Plaintiffs in, but not necessarily
14 limited to, the following ways:

- 15 a) By failing to exercise reasonable care in obtaining, retaining, securing,
16 safeguarding, deleting, and protecting the PII in its possession;
- 17 b) By failing to protect Plaintiffs' PII using reasonable and adequate
18 security procedures and systems that were/are compliant with FTC
19 guidelines and industry-standard practices.
- 20 c) By failing to implement processes to detect the Data Breach, security
21 incidents or intrusions,
- 22 d) By failing to quickly and to timely act on warnings about data
23 breaches;
- 24 e) By failing to timely and promptly notify Plaintiff of any data breach,
25 security incident, or intrusion that affected or may have affected their
26 PII; and
- 27 f) By failing to provide adequate supervision and oversight of the PII
28 with which it was and is entrusted, in spite of the known risk and

foreseeable likelihood of breach and misuse.

78. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

79. To date, Defendant has not provided sufficient information to Plaintiffs regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs.

80. Further, through its failure to provide clear notification of the Data Breach to Plaintiffs, Defendant prevented Plaintiffs from taking meaningful, proactive steps to secure their PII.

81. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the harm suffered, or risk of imminent harm suffered, by Plaintiffs.

82. Defendant's wrongful actions, inactions, and omissions constituted, and continue to constitute, common law negligence.

83. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs have suffered and will suffer injury, including but not limited to:

- a) actual identity theft;
- b) the loss of the opportunity of how their PII is used;
- c) the compromise, publication, and/or theft of their PII;
- d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;
- e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft;
- f) the continued risk to their PII, which may remain in Defendant's

possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' PII in its continued possession; and

g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs.

84. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III: BREACH OF ACTUAL AND IMPLIED CONTRACT (On behalf of all Plaintiffs)

85. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this complaint.

86. Defendant specifically advertised a feature of the service they offer is privacy and security.

87. Plaintiffs believed their PII would be stored and remain private and secure as a condition of purchasing Defendant's services. In so doing, Plaintiffs entered into actual and implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs if their data had been breached and compromised or stolen.

88. At the time Defendant acquired the PII of Plaintiffs, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

89. Implicit in the agreements between Plaintiffs and Defendant to provide PII, was the

1 Defendant's obligation to: (a) use such PII for business purposes only, (b) take
2 reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the
3 PII, (d) retain the PII only under conditions that kept such information secure and
4 confidential, and (e) provide Plaintiffs with prompt and sufficient notice of any and
5 all unauthorized access and/or theft of their PII.

6 90. Plaintiffs fully performed their obligations under the actual and implied contracts
7 with Defendant.

8 91. Defendant breached the actual and implied contracts they made with Plaintiffs by
9 failing to safeguard and protect their personal information, by failing to delete the
10 information that it no longer needed, and by failing to provide timely and accurate
11 notice to them that personal information was compromised as a result of the Data
12 Breach.

13 92. As a direct and proximate result of Defendant's above-described breach of actual
14 and implied contract, Plaintiffs have suffered, and will continue to suffer, ongoing,
15 imminent, and impending threat of identity theft crimes, fraud, and abuse; actual
16 identity theft crimes, fraud, and abuse; loss of the confidentiality of the stolen
17 confidential data; the illegal sale of the compromised data on the dark web;
18 expenses and/or time spent on credit monitoring and identity theft insurance; time
19 spent scrutinizing bank statements, credit card statements, and credit reports;
20 expenses and/or time spent initiating fraud alerts, decreased credit scores and
21 ratings; lost work time; fear, stress, and anxiety; and other economic and non-
22 economic harm.

23 93. As a direct and proximate result of Defendant's above-described breach of actual
24 and implied contract, Plaintiffs are entitled to recover actual, consequential, and
25 nominal damages to be determined at trial.

26 **COUNT IV: INVASION OF PRIVACY – INTRUSION UPON SECLUSION** (On
27 behalf of all Plaintiffs)

28 94. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this

1 complaint.

2 95. Plaintiffs have a legally protected privacy interest in their PII, which is and was
3 collected, stored and maintained by Defendant, and they are entitled to the
4 reasonable and adequate protection of their PII against foreseeable unauthorized
5 access, as occurred with the Data Breach.

6 96. Plaintiffs reasonably expected that Defendant would protect and secure their PII
7 from unauthorized parties and that their PII would not be accessed, removed, and/or
8 disclosed to any unauthorized parties or for any improper purpose.

9 97. Defendant intentionally intruded into Plaintiffs' seclusion by disclosing without
10 permission their PII to a third party. Defendant's acts and omissions giving rise to
11 the Data Breach were intentional in that the decisions to implement lax security and
12 failure to timely notice Plaintiffs were undertaken willfully and intentionally.

13 98. By failing to keep Plaintiffs' PII secure, and disclosing PII to unauthorized parties
14 for unauthorized use, Defendants unlawfully invaded Plaintiffs' privacy right to
15 seclusion by, inter alia:

16 a) invading their privacy by improperly using their PII obtained for a specific
17 purpose for another purpose, or disclosing it to unauthorized persons;

18 b) failing to adequately secure their PII from disclosure to unauthorized persons;
19 and

20 c) enabling the disclosure of their PII without consent.

21 99. This invasion of privacy resulted from Defendant's intentional failure to properly
22 secure and maintain Plaintiffs' PII, leading to the foreseeable unauthorized access,
23 removal, and disclosure of this unguarded and private data.

24 100. Plaintiffs' PII is the type of sensitive, personal information that one normally
25 expects will be protected from exposure by the very entity charged with
26 safeguarding it. Further, the public has no legitimate concern in Plaintiffs' PII, and
27 such information is otherwise protected from exposure to the public by various
28 statutes, regulations and other laws.

1 101. The disclosure of Plaintiffs' PII to unauthorized parties is substantial and
2 unreasonable enough to be legally cognizable and is highly offensive to a
3 reasonable person.

4 102. Defendant's willful and reckless conduct that permitted unauthorized access,
5 removal, and disclosure of Plaintiffs' sensitive PII is such that it would cause
6 serious mental injury, shame or humiliation to people of ordinary sensibilities.

7 103. The unauthorized access, removal, and disclosure of Plaintiffs' PII was without
8 their consent, and in violation of various statutes, regulations, and other laws.

9 104. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiffs
10 suffered injury and sustained actual losses and damages as alleged herein.

11 105. Plaintiffs alternatively seek an award of nominal damages.

12
13 **COUNT V: UNJUST ENRICHMENT** (On behalf of Plaintiffs)

14 106. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this
15 complaint.

16 107. By its wrongful acts and omissions described herein, Defendant has obtained a
17 benefit by unduly taking advantage of Plaintiffs.

18 108. Defendant, prior to and at the time Plaintiffs entrusted their PII to Defendant,
19 caused Plaintiffs to reasonably believe that Defendant would keep such PII secure.

20 109. Defendant was aware, or should have been aware, that reasonable consumers would
21 want their PII secured and would not have contracted with Defendant, directly or
22 indirectly, had they known that Defendant's information systems were substandard
23 for that purpose.

24 110. Defendant was also aware that, if the substandard condition of and vulnerabilities in
25 its information systems were disclosed, it would negatively affect Plaintiffs'
26 decisions to seek services from Defendant.

27 111. Defendant failed to disclose facts pertaining to its substandard information systems,
28 defects, and vulnerabilities therein before Plaintiffs made their decisions to make

1 purchases, engage in commerce therewith, and seek services or information.

2 112. Defendant denied Plaintiffs the ability to make an informed purchasing decision and
3 took undue advantage of Plaintiffs.

4 113. Defendant was unjustly enriched at the expense of Plaintiffs, as Defendant received
5 profits, benefits, and compensation, in part, at the expense of Plaintiffs; however,
6 Plaintiffs did not receive the benefit of their bargain because they paid for services
7 that did not satisfy the purposes for which they bought/sought them.

8 114. Since Defendant's profits, benefits, and other compensation were obtained
9 improperly, Defendant is not legally or equitably entitled to retain any of the
10 benefits, compensation, or profits it realized from these transactions.

11 115. Plaintiffs seek an Order of this Court requiring Defendant to refund, disgorge, and
12 pay as restitution any profits, benefits, and other compensation obtained by
13 Defendant from its wrongful conduct and/or the establishment of a constructive
14 trust from which Plaintiffs may seek restitution.

15 **PRAYER:**

16 Wherefore, Plaintiffs request that this Court award damages and provide relief as
17 follows:

- 18
- 19 A. Pursuant to the Illinois Genetic Information Privacy Act, damages of \$2,500 or
20 actual damages, whichever is greater, for each negligent violation, or \$15,000 or
21 actual damages, whichever is greater, for each intentional or reckless violation, as
22 well as reasonable attorney's fees and costs. 410 Ill. Comp. Stat. Ann. 513/40.
- 23 B. For for all other compensatory damages, statutory damages, punitive damages,
24 restitution, and/or recovery of such relief as permitted by law in kind and amount;
- 25 C. For equitable relief enjoining Defendant from engaging in the wrongful conduct
26 complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' PII,
27 and from refusing to issue prompt, complete, and accurate disclosures to
28 Plaintiffs;

1 D. For injunctive relief requested by Plaintiff, including but not limited to:

- 2 i. prohibiting Defendant from engaging in the wrongful and unlawful acts
3 described herein;
- 4 ii. requiring Defendant to protect, including through encryption, all data
5 collected through the course of business;
- 6 iii. requiring Defendant to delete and purge the PII of Plaintiffs unless
7 Defendant can provide to the Court reasonable justification for the
8 retention and use of such information when weighed against the privacy
9 interests of Plaintiffs;
- 10 iv. requiring Defendant to implement and maintain a comprehensive security
11 program designed to protect the confidentiality and integrity of Plaintiffs'
12 PII;
- 13 v. requiring Defendant to engage independent third-party security auditors
14 and internal personnel to run automated security monitoring, simulated
15 attacks, penetration tests, and audits on Defendant's systems periodically;
- 16 vi. prohibiting Defendant from maintaining Plaintiffs' PII on a cloud-based
17 database;
- 18 vii. requiring Defendant to segment data by creating firewalls and access
19 controls so that, if one area of Defendant's network is compromised,
20 hackers cannot gain access to other portions of Defendant's systems;
- 21 viii. requiring Defendant to conduct regular database scanning and securing
22 checks;
- 23 ix. requiring Defendant to establish an information security training program
24 for all employees, with additional training for employees' responsible for
25 handling PII;
- 26 x. requiring Defendant to implement a system of tests to assess its respective
27 employees' knowledge of the education programs discussed in the
28 preceding subparagraphs, as well as randomly and periodically testing

employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xi. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

xii. requiring Defendant to meaningfully educate Plaintiffs about the threats they face due to the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

E. for pre- and post-judgment interest on all amounts awarded, at the prevailing legal rate;

F. for an award of attorney's fees, costs, and litigation expenses; and

G. for all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiffs hereby demand a trial by jury for all issues triable by jury.

Dated:

POTTER HANDY LLP


By: 
Tehniat Zaman, Esq.
Attorney for Plaintiffs

Exhibit D

Potter Handy, LLP
Mark Potter, Esq., SBN 166317
Barry Walker, Esq., SBN 195947
Jim Treglio, Esq., SBN 228077
Christina Carson, Esq. SBN 280048
Tehniat Zaman, Esq. SBN 321557
Mail: 100 Pine St., Ste. 1250
San Francisco, CA 94111
(415) 534-1911; (888) 422-5191 fax
23andMeIL@potterhandy.com
Attorneys for Plaintiffs

SUPERIOR COURT OF CALIFORNIA
SANTA CLARA COUNTY

CHRISTINA SHAW, et. al.

Plaintiff,

v.

23ANDME, INC.,

Defendant.

Case No.

**COMPLAINT FOR CIVIL
DAMAGES AND INJUNCTIVE
RELIEF**

- 1. Illinois Genetic Information Privacy Act**
- 2. Negligence**
- 3. Breach Of Actual and Implied Contract**
- 4. Invasion Of Privacy – Intrusion Upon Seclusion**
- 5. Unjust Enrichment**

JURY TRIAL DEMANDED

COMPLAINT

Plaintiff; Christina Shaw, et al. (See Attachment 1) (collectively “Plaintiffs”) allege against Defendant 23andMe, Inc. (“23andMe” or “Defendant”) as follows:

SUMMARY:

1. Defendant is a genomic and biotechnology company that looks at an individual's genome for the purpose of creating unique, personalized genetic reports on ancestral origins, personal genetic health risks, chances of passing on carrier conditions, and pharmacogenetics.¹
2. To take advantage of Defendant's services, customers had to provide sensitive personal, genetic, and biological information. To gain the trust of potential customers Defendant expressly advertised the importance of security as "Privacy is in our DNA".
3. On or about October 6, 2023, Defendant announced, via their website, that unauthorized threat actors had accessed 23andMe accounts and compiled customer profile information (the "Data Breach").²
4. The Data Breach contained millions of individuals' private identifying information (hereinafter "PII"), including, but not limited to: names, sex, date of birth, usernames, genetic ancestry, profile photos, geographical locations, living biological relatives, and data about individuals' ethnicity.
5. Plaintiffs are customers of 23andMe that were victims of the Data Breach. Due to the Data Breach, Plaintiffs' PII was released, stolen, and offered for sale on the dark web.
6. Defendant had a non-delegable duty and responsibility to implement and maintain reasonable security measures to secure, safeguard, and protect the private information that it collected, stored, and maintained for Plaintiffs.
7. Defendant disregarded the rights of Plaintiffs by intentionally, willfully, recklessly, or negligently failing to implement adequate and reasonable measures to ensure that Plaintiffs' PII was safeguarded, failing to take all available steps to prevent unauthorized disclosure of data, and failing to follow applicable, and appropriate

¹ <https://www.23andme.com/#> (last visited January 9, 2024).

² <https://blog.23andme.com/articles/addressing-data-security-concerns>

1 protocols, policies, and procedures regarding the encryption of data. The Data
 2 Breach was a direct result of Defendant's failure to implement adequate and
 3 reasonable cyber-security procedures and protocols necessary to protect victims'
 4 PII.

5 8. As a result of Defendant's failure to implement adequate data security measures,
 6 Plaintiffs have suffered actual harm in the disclosure of their PII to unknown and
 7 unauthorized third parties. Plaintiffs have suffered injury and ascertainable losses in
 8 the form of the present and imminent threat of fraud and identity theft, loss of the
 9 benefit of their bargain, out-of-pocket expenses, loss of value of their time
 10 reasonably incurred to remedy or mitigate the effects of the attack, and the loss of,
 11 and diminution in, value of their PII. Plaintiffs also remain vulnerable to future
 12 cyberattacks and thefts from the data in Defendant's possession.

13 9. As such, Plaintiffs assert claims for Illinois Genetic Information Privacy Act
 14 (GIPA), 410 ILCS 513 *et seq.*; negligence, breach of implied contract, invasion of
 15 privacy, and unjust enrichment.

16 **JURISDICTION AND VENUE:**

17 10. This Court has subject matter jurisdiction over this action pursuant to Article VI,
 18 section 10 of the California Constitution and Code of Civil Procedure section
 19 410.10

20 11. This Court has personal jurisdiction over Defendant because it is headquartered in
 21 the State of California, county of Santa Clara, and purposefully avails itself of the
 22 laws, protections, and advantages of this State.

23 12. Venue is proper in this Court because Defendant conducts business in this County
 24 and reaped substantial profits from customers in this County. In addition, in its own
 25 Terms of Service, Defendant has agreed "...to submit to the exclusive jurisdiction
 26 of any state or federal court located in Santa Clara County, California (except for
 27 small claims court actions which may be brought in the county where you reside),
 28 and waive any jurisdictional, venue, or inconvenient forum objections to such

courts.” Finally, a substantial part of the acts and conduct charged herein occurred in this County.

PARTIES:

13. Plaintiffs are residents of Illinois who provided 23andMe with a DNA sample for analysis and whose private identifying information was compromised by the Data Breach.
14. Defendant 23andMe, Inc. is a biotechnology company headquartered in California that collects and analyzes an individual’s genome for the purpose of creating personalized genetic reports directly to consumers.

FACTUAL ALLEGATIONS:

Defendant collected and stored Plaintiffs’ PII

15. Defendant collects PII from their customers in the course of doing business.
16. As a condition of receiving Defendant’s services, Plaintiffs were required to entrust Defendant with highly sensitive genetic information, information derived from genetic testing, health information, ancestral origin, and other confidential and sensitive PII. 23andMe then stores that information in its platform.
17. According to the Privacy Statement on 23andMe’s website, the company collects the following categories of customer information:
 - a) Registration Information, including name, user ID, password, date of birth, billing address, shipping address, payment information, account authentication information, and contact information (such as email address and phone number).
 - b) Genetic information, including “[i]nformation regarding your genotype (e.g., the As, Ts, Cs, and Gs at particular locations in your DNA)” and “the 23andMe genetic data and reports provided to you as part of our Services.”
 - c) Sample Information, including “[i]nformation regarding any sample, such as a saliva sample, that you submit for processing to be analyzed to provide you with

Genetic Information, laboratory values or other data provided through our Services.”

d) Self-Reported Information, including “gender, disease conditions, health related information, traits, ethnicity, family history, or anything else you want to provide to us within our Service(s).”

e) User Content, including “[i]nformation, data, text, software, music, audio, photographs, graphics, video, messages, or other materials, other than Genetic Information and Self-Reported Information, generated by users of 23andMe Services and transmitted, whether publicly or privately, to or through 23andMe. For example, User Content includes comments posted on our Blog or messages you send through our Services.”

f) Web-Behavior Information, including “[i]nformation on how you use our Services or about the way your devices use our Services is collected through log files, cookies, web beacons, and similar technologies (e.g., device information, device identifiers, IP address, browser type, location, domains, page views).”

g) Biometric Information, including “[c]ertain Self-Reported Information you provide to us or our service providers to verify your identity using biological characteristics.”

18. As part of its advertising, Defendant promises to maintain the confidentiality of Plaintiffs’ PII to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiffs’ PII for non-essential purposes.

19. Defendant’s Privacy Policy states that it “encrypt[s] all sensitive information and conduct[s] regular assessments to identify security vulnerabilities and threats.”³

20. By obtaining, collecting, using, and deriving a benefit from Plaintiffs’ PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs’ PII from unauthorized disclosure.

21. Additionally, Defendant had and continues to have obligations created by applicable

³ <https://www.23andme.com/privacy/>

1 state law, reasonable industry standards, common law, and its own assurances and
2 representations to keep Plaintiffs' PII confidential and to protect such PII from
3 unauthorized access.

4 22. Defendant created the reasonable expectation and mutual understanding with
5 Plaintiffs that it would comply with its obligations to Plaintiffs' information,
6 including the PII, confidential and secure from unauthorized access.

7 23. Plaintiffs have the utmost privacy interest in the highly sensitive nature of PII, and
8 would not have been induced to purchase the genetic testing offered by Defendant
9 had Defendant not included privacy assurances within its advertising.

10 24. Plaintiffs took reasonable steps to maintain the confidentiality of their PII and relied
11 on Defendant to keep their PII confidential and securely maintained, to use this
12 information for business purposes only, and to make only authorized disclosures of
13 this information.

14
15 ***Data Breach***

16 25. On October 6, 2023, Defendant revealed that threat actors were able to access
17 customer accounts and obtain customers' PII without authorization and consent.

18 26. Despite the prevalence of public announcements of data breach and data security
19 compromises in recent years, Defendant failed to take sufficient steps to protect
20 Plaintiffs' PII from being compromised.

21 27. Upon information and belief, Defendant did not require two-factor authentication to
22 protect Plaintiffs' PII at the time of the Data Breach.

23 28. Upon information and belief, Defendant did not adequately monitor, secure, and/or
24 encrypt its servers and Plaintiffs' PII.

25 29. Upon information and belief, Defendant could have prevented the Data Breach.

26 30. Upon information and belief, the cyberattack was expressly designed to gain access
27 to private and confidential data, including Plaintiffs' PII.

28 31. Due to Defendant's inadequate security measures, Plaintiffs now face a present,

1 immediate, and ongoing risk of fraud and identity theft and must deal with that
2 threat indefinitely.

3
4 ***Defendant failed to adequately protect the PII and failed to timely notify Plaintiffs their***
5 ***data had been compromised***

6 32. On November 6, 2023—one month after it disclosed the breach—23andMe
7 announced that it was “requiring all customers use a second step of verification to
8 sign into their account.”

9 33. On information and belief, Defendant did not begin notifying Plaintiffs their
10 specific PII had been compromised until on or after December 1, 2023.

11 34. On information and belief, Defendant continues to fail to take reasonable and
12 adequate measure to notify all impacted customers that their PII has been
13 compromised.

14 35. At all relevant times, Defendant had a duty to exercise reasonable care in obtaining,
15 retaining, securing, safeguarding, deleting, and protecting the PII in Defendant’s
16 possession from being compromised, lost, stolen, accessed, and misused by
17 unauthorized persons.

18 36. At all relevant times, Defendant had a duty to properly secure the collected PII,
19 encrypt and maintain such information using industry standard methods, create and
20 implement reasonable data security practices and procedures, train its employees,
21 utilize available technology to defend its systems from invasion, act reasonably to
22 prevent foreseeable harm to Plaintiffs, and to promptly notify Plaintiffs when
23 Defendant became aware that Plaintiffs’ PII may have been compromised.

24 37. Defendant touted its security and privacy as part of their advertising. Defendant’s
25 duty to use reasonable security measures arose as a result of the Plaintiffs’
26 reasonable reliance on Defendant to secure their highly sensitive personal data.
27 Plaintiffs surrendered the data to obtain Defendant’s services under the express
28 condition that Defendant would keep it private and secure. Accordingly, Defendant

also has a duty to safeguard their data, independent of any statute.

38. Defendant owed a duty of care to Plaintiffs because they were foreseeable and probable victims of any inadequate data security practices.

Value of the PII

39. PII are highly valuable for identity thieves and personal information is sold on several underground internet websites for \$40 to \$200⁴ per identity.

40. Identity thieves can use PII, such as that of Plaintiffs to perpetrate a variety of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

41. Criminals can also use stolen PII to extort a financial payment by leveraging sensitive healthcare information, for example a sexually transmitted disease or terminal illness, to extort or coerce the victim.

42. Familial relationships and ethnic background can be used to target certain minority groups with threats or even violence.

43. Data breaches involving medical information are more difficult to detect, and take longer to uncover, than normal identity theft. In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief can use private information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."⁵ The FTC also warns that if a thief's health information is mixed with the victim's it "could affect the medical care [they are] able to get or the health insurance benefits [they are]

⁴ Anita George, DIGITAL TRENDS, Your personal data is for sale on the dark web. Here's how much it costs (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

⁵ See What to Know About Medical Identity Theft, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last visited Oct. 2, 2023).

1 able to use.”⁶

2 44. Defendant is a large, sophisticated organization with the resources to deploy robust
3 cybersecurity protocols. It knew, or should have known, that the development and
4 use of such protocols were necessary to fulfill its statutory and common law duties
5 to Plaintiffs. It knew, or should have known, that PII is sought after and valuable
6 target for thieves and that there was a high likelihood this information would be
7 targeted. Therefore, its failure to do so is intentional, willful, reckless, and/or
8 grossly negligent.

9 45. Defendant disregarded the rights of Plaintiffs by, inter alia, (i) intentionally,
10 willfully, recklessly, or negligently failing to take adequate and reasonable measures
11 to ensure that its network servers were protected against unauthorized intrusions;
12 (ii) failing to disclose that it did not have adequately robust security protocols and
13 training practices in place to adequately safeguard Plaintiffs’ PII; (iii) failing to take
14 standard and reasonably available steps to prevent the Data Breach; (iv) concealing
15 the existence and/or extent of the Data Breach for an unreasonable duration of time;
16 and (v) failing to provide Plaintiff prompt and accurate notice of the Data Breach.

17 46. Plaintiffs have suffered lost time, annoyance, interference, and inconvenience as a
18 result of the Data Breach and have fear, stress, anxiety and increased concerns for
19 the loss of their privacy and PII being in the hands of criminals.

20 47. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and
21 money on an ongoing basis to try to mitigate and address harms caused by the Data
22 Breach.

23 48. As a result of the Data Breach, Plaintiffs are at risk and will continue to be at
24 increased risk of identity theft and fraud for years to come.

25 49. Plaintiffs have a continuing interest in ensuring that their Private Information, which,
26 upon information and belief, remains backed up in Defendant’s possession, is
27 protected and safeguarded from future breaches.

28 ⁶ *Id.*

Defendant Fails to Comply with FTC Guidelines

50. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

51. FTC guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.

52. The guidelines also recommend companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures. Further, it recommends businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.⁷

53. The FTC guidelines also form part of the basis of Defendant’s duty in this regard.

54. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its customers, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs.

Injuries and Damages:

⁷ Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 2, 2023).

1 55. As a result of the Data Breach, Plaintiffs have all sustained actual injuries and
 2 damages, including: (i) lost or diminished value of their PII; (ii) lost opportunity
 3 costs associated with attempting to mitigate the actual consequences of the Data
 4 Breach, including but not limited to lost time; (iii) lost time spent on activities
 5 remedying harms resulting from the Data Breach; (iv) invasion of privacy; (v) loss
 6 of benefit of the bargain; (vi) the continued and certainly increased risk to their PII;
 7 and (vii) fear, stress, and anxiety.

8 56. The information disclosed in this Data Breach is impossible to change. Plaintiffs
 9 will have to monitor for identity theft and breaches their entire lives. The retail cost
 10 of credit monitoring and identity theft monitoring can cost around \$200 a year per
 11 Plaintiff. This is a reasonable and necessary cost to monitor to protect Plaintiffs
 12 from the risk of identity theft that arose from the Data Breach. This is a future cost
 13 that Plaintiffs would not need to bear but for Defendant's failure to safeguard their
 14 PII.

CLAIMS FOR RELIEF:

COUNT I: Illinois Genetic Information Privacy Act (On behalf of all Plaintiffs).

17 57. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this
 18 complaint.

19 58. The Genetic Information Privacy Act (GIPA), 410 Ill. Comp. Stat. Ann. 513 *et seq.*,
 20 covers "[c]onfidentiality of genetic information" and provides in relevant part:
 21 "Except as otherwise provided in this Act, genetic testing and information derived
 22 from genetic testing is confidential and privileged and may be released only to the
 23 individual tested and to persons specifically authorized, in writing in accordance
 24 with Section 30, by that individual to receive the information." 410 Ill. Comp. Stat.
 25 Ann. 513/15(a).

26 59. GIPA incorporates the definition of "genetic information" from 45 C.F.R. §
 27 160.103, which defines the term as "information about" an individual's "genetic
 28 tests," "[t]he genetic tests of family members of the individual," "[t]he

1 manifestation of a disease or disorder in family members of such individual,” or
2 “[a]ny request for, or receipt of, genetic services, or participation in clinical research
3 which includes genetic services, by the individual or any family member of the
4 individual.”

5 60. GIPA also incorporates the definition of “genetic test” from 45 C.F.R. § 160.103,
6 which defines the term as “an analysis of human DNA, RNA, chromosomes,
7 proteins, or metabolites, if the analysis detects genotypes, mutations, or
8 chromosomal changes.”

9 61. The test performed by 23andMe qualifies as “genetic testing” under GIPA because
10 it detects, inter alia, genotypes and mutations.

11 62. The information compromised in the breach of 23andMe’s platform included
12 genetic information, genetic testing, and information derived from such
13 information. For example, the origin of Plaintiffs’ ancestors, the list of other
14 23andMe users identified by 23andMe as Plaintiff’s DNA relatives, and the
15 information on the number of DNA segments Plaintiffs shared with those other
16 users were all information about, and derived from, the 23andMe genetic test
17 Plaintiff purchased. Moreover, these results serve as a receipt of genetic services
18 performed by 23andMe for Plaintiff.

19 63. 23andMe negligently and recklessly released Plaintiff and class members’ genetic
20 information, PII, and other confidential and highly sensitive PII by failing to
21 adequately safeguard that information from malicious actors. Considering the
22 number of data breaches and the sensitivity of the information it possessed,
23 23andMe was aware or should have been aware of the need to implement robust
24 security measures to protect such information. It consciously refused to do so.

25 64. By negligently and recklessly releasing Plaintiffs’ information (including genetic
26 testing and information derived from genetic testing performed by 23andMe) to
27 unauthorized parties, as alleged above, 23andMe violated GIPA.

28 65. Accordingly, Plaintiffs are entitled to, and seek, damages of “\$2,500 or actual

1 damages, whichever is greater,” for each negligent violation, or “\$15,000 or actual
2 damages, whichever is greater,” for each intentional or reckless violation, as well as
3 reasonable attorney’s fees and costs. 410 Ill. Comp. Stat. Ann. 513/40.

4 66. Plaintiffs are also authorized to obtain injunctive relief to prevent future violations.
5 *Id.*

6
7 **COUNT II: Negligence** (On behalf of all Plaintiffs).

8 67. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this
9 complaint.

10 68. At all times herein relevant, Defendant owed Plaintiffs a duty of care, *inter alia*, to
11 act with reasonable care to secure and safeguard their PII and to use commercially
12 reasonable methods to do so. Defendant took on this obligation upon accepting and
13 storing the PII of Plaintiffs in its computer systems and on its networks.

14 69. Defendant knew that the PII was private and confidential and should be protected
15 and, thus, Defendant owed a duty of care not to subject Plaintiffs to an unreasonable
16 risk of harm because they were foreseeable and probable victims of any inadequate
17 security practices.

18 70. Defendant knew, or should have known, of the risks inherent in collecting and
19 storing PII, the vulnerabilities of its data security systems, and the importance of
20 adequate security.

21 71. Defendant knew, or should have known, that its data systems and networks did not
22 adequately safeguard Plaintiffs’ PII.

23 72. Only Defendant was in the position to ensure that its systems and protocols were
24 sufficient to protect the PII that Plaintiffs had entrusted to it.

25 73. Because Defendant knew that a breach of its systems could damage thousands of
26 individuals, including Plaintiffs, Defendant had a duty to adequately protect its data
27 systems and the PII contained therein.

28 74. Plaintiffs’ willingness to entrust Defendant with their PII was predicated on the

1 understanding that Defendant would take adequate security precautions.

2 75. Moreover, only Defendant had the ability to protect its systems and the PII stored
3 on them from attack.

4 76. Defendant also had independent duties under state laws that required Defendant to
5 reasonably safeguard Plaintiffs' PII and promptly notify them about the Data
6 Breach. These "independent duties" are untethered to any contract between
7 Defendant and Plaintiffs.

8 77. Defendant breached its general duty of care to Plaintiffs in, but not necessarily
9 limited to, the following ways:

10 a) By failing to exercise reasonable care in obtaining, retaining, securing,
11 safeguarding, deleting, and protecting the PII in its possession;

12 b) By failing to protect Plaintiffs' PII using reasonable and adequate
13 security procedures and systems that were/are compliant with FTC
14 guidelines and industry-standard practices.

15 c) By failing to implement processes to detect the Data Breach, security
16 incidents or intrusions,

17 d) By failing to quickly and to timely act on warnings about data
18 breaches;

19 e) By failing to timely and promptly notify Plaintiff of any data breach,
20 security incident, or intrusion that affected or may have affected their
21 PII; and

22 f) By failing to provide adequate supervision and oversight of the PII
23 with which it was and is entrusted, in spite of the known risk and
24 foreseeable likelihood of breach and misuse.

25 78. Defendant's willful failure to abide by these duties was wrongful, reckless, and
26 grossly negligent in light of the foreseeable risks and known threats.

27 79. To date, Defendant has not provided sufficient information to Plaintiffs regarding
28 the extent of the unauthorized access and continues to breach its disclosure

obligations to Plaintiffs.

80. Further, through its failure to provide clear notification of the Data Breach to Plaintiffs, Defendant prevented Plaintiffs from taking meaningful, proactive steps to secure their PII.

81. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the harm suffered, or risk of imminent harm suffered, by Plaintiffs.

82. Defendant's wrongful actions, inactions, and omissions constituted, and continue to constitute, common law negligence.

83. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs have suffered and will suffer injury, including but not limited to:

- a) actual identity theft;
- b) the loss of the opportunity of how their PII is used;
- c) the compromise, publication, and/or theft of their PII;
- d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;
- e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft;
- f) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' PII in its continued possession; and
- g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII

1 compromised as a result of the Data Breach for the remainder of the
2 lives of Plaintiffs.

3 84. As a direct and proximate result of Defendant's negligence and negligence per se,
4 Plaintiffs have suffered and will continue to suffer other forms of injury and/or
5 harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and
6 other economic and non-economic losses.

7
8 **COUNT III: BREACH OF ACTUAL AND IMPLIED CONTRACT** (On behalf of
9 all Plaintiffs)

10 85. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this
11 complaint.

12 86. Defendant specifically advertised a feature of the service they offer is privacy and
13 security.

14 87. Plaintiffs believed their PII would be stored and remain private and secure as a
15 condition of purchasing Defendant's services. In so doing, Plaintiffs entered into
16 actual and implied contracts with Defendant by which Defendant agreed to
17 safeguard and protect such information, to keep such information secure and
18 confidential, and to timely and accurately notify Plaintiffs if their data had been
19 breached and compromised or stolen.

20 88. At the time Defendant acquired the PII of Plaintiffs, there was a meeting of the
21 minds and a mutual understanding that Defendant would safeguard the PII and not
22 take unjustified risks when storing the PII.

23 89. Implicit in the agreements between Plaintiffs and Defendant to provide PII, was the
24 Defendant's obligation to: (a) use such PII for business purposes only, (b) take
25 reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the
26 PII, (d) retain the PII only under conditions that kept such information secure and
27 confidential, and (e) provide Plaintiffs with prompt and sufficient notice of any and
28 all unauthorized access and/or theft of their PII.

1 90. Plaintiffs fully performed their obligations under the actual and implied contracts
2 with Defendant.

3 91. Defendant breached the actual and implied contracts they made with Plaintiffs by
4 failing to safeguard and protect their personal information, by failing to delete the
5 information that it no longer needed, and by failing to provide timely and accurate
6 notice to them that personal information was compromised as a result of the Data
7 Breach.

8 92. As a direct and proximate result of Defendant's above-described breach of actual
9 and implied contract, Plaintiffs have suffered, and will continue to suffer, ongoing,
10 imminent, and impending threat of identity theft crimes, fraud, and abuse; actual
11 identity theft crimes, fraud, and abuse; loss of the confidentiality of the stolen
12 confidential data; the illegal sale of the compromised data on the dark web;
13 expenses and/or time spent on credit monitoring and identity theft insurance; time
14 spent scrutinizing bank statements, credit card statements, and credit reports;
15 expenses and/or time spent initiating fraud alerts, decreased credit scores and
16 ratings; lost work time; fear, stress, and anxiety; and other economic and non-
17 economic harm.

18 93. As a direct and proximate result of Defendant's above-described breach of actual
19 and implied contract, Plaintiffs are entitled to recover actual, consequential, and
20 nominal damages to be determined at trial.

21 **COUNT IV: INVASION OF PRIVACY – INTRUSION UPON SECLUSION** (On
22 behalf of all Plaintiffs)

23 94. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this
24 complaint.

25 95. Plaintiffs have a legally protected privacy interest in their PII, which is and was
26 collected, stored and maintained by Defendant, and they are entitled to the
27 reasonable and adequate protection of their PII against foreseeable unauthorized
28 access, as occurred with the Data Breach.

- 1 96. Plaintiffs reasonably expected that Defendant would protect and secure their PII
2 from unauthorized parties and that their PII would not be accessed, removed, and/or
3 disclosed to any unauthorized parties or for any improper purpose.
- 4 97. Defendant intentionally intruded into Plaintiffs' seclusion by disclosing without
5 permission their PII to a third party. Defendant's acts and omissions giving rise to
6 the Data Breach were intentional in that the decisions to implement lax security and
7 failure to timely notice Plaintiffs were undertaken willfully and intentionally.
- 8 98. By failing to keep Plaintiffs' PII secure, and disclosing PII to unauthorized parties
9 for unauthorized use, Defendants unlawfully invaded Plaintiffs' privacy right to
10 seclusion by, inter alia:
- 11 a) invading their privacy by improperly using their PII obtained for a specific
12 purpose for another purpose, or disclosing it to unauthorized persons;
- 13 b) failing to adequately secure their PII from disclosure to unauthorized persons;
14 and
- 15 c) enabling the disclosure of their PII without consent.
- 16 99. This invasion of privacy resulted from Defendant's intentional failure to properly
17 secure and maintain Plaintiffs' PII, leading to the foreseeable unauthorized access,
18 removal, and disclosure of this unguarded and private data.
- 19 100. Plaintiffs' PII is the type of sensitive, personal information that one normally
20 expects will be protected from exposure by the very entity charged with
21 safeguarding it. Further, the public has no legitimate concern in Plaintiffs' PII, and
22 such information is otherwise protected from exposure to the public by various
23 statutes, regulations and other laws.
- 24 101. The disclosure of Plaintiffs' PII to unauthorized parties is substantial and
25 unreasonable enough to be legally cognizable and is highly offensive to a
26 reasonable person.
- 27 102. Defendant's willful and reckless conduct that permitted unauthorized access,
28 removal, and disclosure of Plaintiffs' sensitive PII is such that it would cause

serious mental injury, shame or humiliation to people of ordinary sensibilities.

103. The unauthorized access, removal, and disclosure of Plaintiffs' PII was without their consent, and in violation of various statutes, regulations, and other laws.

104. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiffs suffered injury and sustained actual losses and damages as alleged herein.

105. Plaintiffs alternatively seek an award of nominal damages.

COUNT V: UNJUST ENRICHMENT (On behalf of Plaintiffs)

106. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this complaint.

107. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiffs.

108. Defendant, prior to and at the time Plaintiffs entrusted their PII to Defendant, caused Plaintiffs to reasonably believe that Defendant would keep such PII secure.

109. Defendant was aware, or should have been aware, that reasonable consumers would want their PII secured and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were substandard for that purpose.

110. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiffs' decisions to seek services from Defendant.

111. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiffs made their decisions to make purchases, engage in commerce therewith, and seek services or information.

112. Defendant denied Plaintiffs the ability to make an informed purchasing decision and took undue advantage of Plaintiffs.

113. Defendant was unjustly enriched at the expense of Plaintiffs, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiffs; however,

1 Plaintiffs did not receive the benefit of their bargain because they paid for services
2 that did not satisfy the purposes for which they bought/sought them.

3 114. Since Defendant's profits, benefits, and other compensation were obtained
4 improperly, Defendant is not legally or equitably entitled to retain any of the
5 benefits, compensation, or profits it realized from these transactions.

6 115. Plaintiffs seek an Order of this Court requiring Defendant to refund, disgorge, and
7 pay as restitution any profits, benefits, and other compensation obtained by
8 Defendant from its wrongful conduct and/or the establishment of a constructive
9 trust from which Plaintiffs may seek restitution.

10 **PRAYER:**

11 Wherefore, Plaintiffs request that this Court award damages and provide relief as
12 follows:

- 13 A. Pursuant to the Illinois Genetic Information Privacy Act, damages of \$2,500 or
14 actual damages, whichever is greater, for each negligent violation, or \$15,000 or
15 actual damages, whichever is greater, for each intentional or reckless violation, as
16 well as reasonable attorney's fees and costs. 410 Ill. Comp. Stat. Ann. 513/40.
17 B. For for all other compensatory damages, statutory damages, punitive damages,
18 restitution, and/or recovery of such relief as permitted by law in kind and amount;
19 C. For equitable relief enjoining Defendant from engaging in the wrongful conduct
20 complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' PII,
21 and from refusing to issue prompt, complete, and accurate disclosures to
22 Plaintiffs;
23 D. For injunctive relief requested by Plaintiff, including but not limited to:
24 i. prohibiting Defendant from engaging in the wrongful and unlawful acts
25 described herein;
26 ii. requiring Defendant to protect, including through encryption, all data
27 collected through the course of business;
28

- 1 iii. requiring Defendant to delete and purge the PII of Plaintiffs unless
- 2 Defendant can provide to the Court reasonable justification for the
- 3 retention and use of such information when weighed against the privacy
- 4 interests of Plaintiffs;
- 5 iv. requiring Defendant to implement and maintain a comprehensive security
- 6 program designed to protect the confidentiality and integrity of Plaintiffs’
- 7 PII;
- 8 v. requiring Defendant to engage independent third-party security auditors
- 9 and internal personnel to run automated security monitoring, simulated
- 10 attacks, penetration tests, and audits on Defendant’s systems periodically;
- 11 vi. prohibiting Defendant from maintaining Plaintiffs’ PII on a cloud-based
- 12 database;
- 13 vii. requiring Defendant to segment data by creating firewalls and access
- 14 controls so that, if one area of Defendant’s network is compromised,
- 15 hackers cannot gain access to other portions of Defendant’s systems;
- 16 viii. requiring Defendant to conduct regular database scanning and securing
- 17 checks;
- 18 ix. requiring Defendant to establish an information security training program
- 19 for all employees, with additional training for employees’ responsible for
- 20 handling PII;
- 21 x. requiring Defendant to implement a system of tests to assess its respective
- 22 employees’ knowledge of the education programs discussed in the
- 23 preceding subparagraphs, as well as randomly and periodically testing
- 24 employees’ compliance with Defendant’s policies, programs, and systems
- 25 for protecting PII;
- 26 xi. requiring Defendant to implement, maintain, review, and revise as
- 27 necessary a threat management program to monitor Defendant’s networks
- 28 for internal and external threats appropriately, and assess whether

- 1 monitoring tools are properly configured, tested, and updated; and
- 2 xii. requiring Defendant to meaningfully educate Plaintiffs about the threats
- 3 they face due to the loss of their confidential PII to third parties, as well as
- 4 the steps affected individuals must take to protect themselves;
- 5 E. for pre- and post-judgment interest on all amounts awarded, at the prevailing legal
- 6 rate;
- 7 F. for an award of attorney's fees, costs, and litigation expenses; and
- 8 G. for all other Orders, findings, and determinations identified and sought in this
- 9 Complaint.

10


11 **JURY DEMAND**

12 Plaintiffs hereby demand a trial by jury for all issues triable by jury.

13

14 Dated: July 8, 2024

POTTER HANDY LLP

15 By: 

16 Tehniat Zaman, Esq.

17 Attorney for Plaintiffs

18

19

20

21

22

23

24

25

26

27

28

Exhibit E

1 Mark N. Todzo (Bar No. 168389)
2 **LEXINGTON LAW GROUP**
3 503 Divisadero Street
4 San Francisco, CA 94117
5 Telephone: 415-913-7800
6 Facsimile: 415-759-4112
7 mtodzo@lexlawgroup.com

8 *Attorneys for Plaintiff*

9 [Additional Counsel on Signature Page.]

10
11 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
12 **COUNTY OF SAN FRANCISCO**

13 MARJORIE MORGENSTERN on Behalf of
14 Herself and All Others Similarly Situated,

15 Plaintiff,

16 v.

17 23ANDME HOLDING CO. and 23ANDME,
18 INC.,

19 Defendants.

Case No. CGC-23-610816

CLASS ACTION

**NOTICE OF SUBMISSION OF
PETITION FOR COORDINATION**

TO ALL PARTIES AND TO THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that, pursuant to Rule 3.522 of the California Rules of Court (“C.R.C.”), notice is hereby given that on January 25, 2024, Marjorie Morgenstern (“Petitioner”) submitted a Petition for Coordination to the Chair of the Judicial Council seeking to coordinate the following actions:

1. *Morgenstern v. 23andMe Holding Co., et al.* (San Francisco Case No. 23-610816) (the “*Morgenstern* Action”); and
2. *Vasquez v. 23andMe, Inc.*, (Santa Clara Case No. 23CV424996) (the “*Vasquez* Action”).

In addition, Petitioner submitted a request that the Judicial Council stay all proceedings in the *Vasquez* Action. Copies of the Petition for Coordination, together with the Declaration of Mark N. Todzo, Memorandum of Points and Authorities, and Application for Stay Order, submitted therewith, are attached hereto as Exhibits A-D.

Petitioner is represented by Mark N. Todzo of the Lexington Law Group, whose address is 503 Divisadero Street, San Francisco, California 94117.

Pursuant to C.R.C. Rule 3.522(a)(4), you are hereby advised that if you intend to oppose the Petition for Coordination you must serve and submit an opposition thereto at least nine court days before the hearing date.

Dated: January 25, 2024

LEXINGTON LAW GROUP



Mark N. Todzo (Bar No. 168389)
Patrick R. Carey (Bar No. 308623)
Meredyth L. Merrow (Bar No. 328337)
503 Divisadero Street
San Francisco, CA 94117

1 Telephone: (415) 913-7800
2 Facsimile: (415) 759-4112
3 mtodzo@lexlawgroup.com

4 Joseph P. Guglielmo (*pro hac vice* forthcoming)
5 Carey Alexander (*pro hac vice* forthcoming)
6 **SCOTT+SCOTT ATTORNEYS AT LAW LLP**
7 The Helmsley Building
8 230 Park Avenue, 17th Floor
9 New York, NY 10169-1820
10 Telephone: (212) 223-6444
11 Facsimile: (212) 223-6334
12 jguglielmo@scott-scott.com
13 calexander@scott-scott.com

14 *Attorneys for Plaintiff*
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Exhibit A

RECEIVED

Judicial Council of California

JAN 24 2024

Coordination Lawyer

Mark N. Todzo (Bar No. 168389)
LEXINGTON LAW GROUP
503 Divisadero Street
San Francisco, CA 94117
Telephone: 415-913-7800
Facsimile: 415-759-4112
mtodzo@lexlawgroup.com

Attorneys for Petitioner

[Additional Counsel on Signature Page.]

JUDICIAL COUNCIL OF THE STATE OF CALIFORNIA

IN THE MATTER OF THE REQUEST FOR
COORDINATION OF THE FOLLOWING
ACTIONS:

IN THE SUPERIOR COURT FOR THE
COUNTY OF SAN FRANCISCO (Case No.
CGC-23-610816)

MARJORIE MORGENSTERN on Behalf of
Herself and All Others Similarly Situated,

Plaintiff,

v.

23ANDME HOLDING CO. and 23ANDME,
INC.,

Defendants.

IN THE SUPERIOR COURT FOR THE
COUNTY OF SANTA CLARA (Case No.
23CV424996):

KATHY VASQUEZ, Individually and on Behalf
of All Others Similarly Situated,

Plaintiff,

v.

23ANDME, INC.,

Defendant.

Judicial Counsel Coordination Proceeding
No. **5315**

PETITION FOR COORDINATION

[Filed concurrently with MPA ISO
Petition for Coordination; Declaration of
Mark N. Todzo; Application for Stay
Order]

HEARING REQUESTED

1 TO: CHAIRMAN OF THE JUDICIAL COUNCIL, STATE OF CALIFORNIA

2 Petitioner Marjorie Morgenstern (“Petitioner”) is the sole plaintiff in *Morgenstern v.*
3 *23andMe Holding Co., et al.*, San Francisco County Superior Court Case No. 23-610816, and
4 therefore, pursuant to California Civil Procedure Code (“C.C.P.”) §404, *et seq.*, and California
5 Rules of Court (“C.R.C.”) Rule 3.521, Petitioner requests that a judge be assigned to determine
6 whether coordination of the two above-captioned actions (“Included Actions”) is appropriate. This
7 Petition for Coordination (the “Petition”) is based upon the Memorandum of Points and Authorities
8 filed herewith, the Declaration of Mark N. Todzo filed herewith, and all of the papers, pleadings,
9 and files in the Included Actions. This Petition is made on the grounds that the Included Actions
10 share common questions of both fact and law and that coordination will promote the ends of
11 justice. Pursuant to C.R.C. Rule 3.521(a), Petitioner requests that the Petition be set for hearing if
12 there is any opposition to this Petition.

13 1. The name of the Petitioner is Marjorie Morgenstern. Petitioner is represented by
14 Mark N. Todzo of the Lexington Law Group, located at 503 Divisadero Street, San Francisco,
15 California, 94117.

16 2. The names of the parties in the Included Actions and the name and address of each
17 party’s attorney of record, if any, are as follows:

18 (a) *Morgenstern v. 23andMe Holding Co., et al.* (San Francisco Case No. 23-
19 610816) (the “*Morgenstern* Action”)

COUNSEL	PARTY OR PARTIES REPRESENTED
Mark N. Todzo Patrick R. Carey Meredyth L. Merrow LEXINGTON LAW GROUP 503 Divisadero Street San Francisco, CA 94117 Telephone: (415) 913-7800 Facsimile: (415) 759-4112 mtodzo@lexlawgroup.com Joseph P. Guglielmo Carey Alexander SCOTT+SCOTT ATTORNEYS AT LAW LLP The Helmsley Building 230 Park Avenue, 17th Floor New York, NY 10169-1820 Telephone: (212) 223-6444 Facsimile: (212) 223-6334 jguglielmo@scott-scott.com calexander@scott-scott.com	Plaintiff Marjorie Morgenstern
No appearance to date	Defendants 23andMe Holding Co., and 23andMe, Inc.

(b) *Vasquez v. 23andMe, Inc.*, (Santa Clara Case No. 23CV424996) (the “*Vasquez Action*”)

COUNSEL	PARTY OR PARTIES REPRESENTED
Jason M. Wucetich Dimitrios V. Korovilas WUCETICH & KOROVILAS LLP 222 N. Pacific Coast Hwy., Suite 2000 El Segundo, CA 90245 Telephone: (310) 335-2001 Facsimile: (310) 364-5201 jason@wukolaw.com dimitri@wukolaw.com	Plaintiff Kathy Vasquez
No appearance to date	Defendant 23andMe, Inc.

3. Petitioner has served the summons and operative complaint on all defendants in the *Morgenstern Action*. Petitioner is unaware of the status of service in the *Vasquez Action*.

4. The complete title and case number of each case known by Petitioner to be a related case pending in a court of the State of California that is subject to coordination, the court in which such case is pending, and the filing date of each, are as follows:

(a) Marjorie Morgenstern on Behalf of Herself and All Others Similarly Situated
Plaintiff,

v.

23andMe Holding Co. and 23andMe, Inc.,
Defendants

San Francisco Superior Court Case No. CGC-23-610816, filed December 4, 2023; and

(b) Kathy Vasquez, individually and on behalf of all others similarly situated,
Plaintiff,

v.

23andMe, Inc.,
Defendant

Santa Clara Superior Court Case No. 23CV424996, filed October 31, 2023.

5. Petitioner knows of no other actions pending in a California court that share predominating common questions of fact or law with the Included Actions.

6. Petitioner is informed and believes, and upon such information and belief, states that the status of each Included Action is as follows:

(a) Petitioner filed the *Morgenstern* Action on December 4, 2023, in San Francisco County Superior Court. The *Morgenstern* Action asserts eight claims for relief against two distinct 23andMe entities – 23andMe Holding Co., and 23andMe Inc. – flowing from 23andMe’s exposure of Petitioner’s personal identifiable information (“PII”) and personal genetic and health information (“PGI”). The summons was issued on December 6, 2023, and the executed proof of service was filed on January 9, 2024. On December 15, 2023, Petitioner filed a Notice of

1 Related Cases indicating the *Morgenstern* Action’s relation to cases pending in Federal Court in the
2 Northern District of California. On December 19, 2023, Petitioner filed an application to designate
3 the *Morgenstern* Action as complex, which remains pending. An initial case management
4 conference has been set for May 8, 2024.

5 (b) Kathy Vasquez (“Vasquez”) filed the *Vasquez* Action on October 31, 2023,
6 in Santa Clara Superior Court. That same day, the Court set an initial case management conference
7 for March 14, 2024. While the summons was issued on October 31, 2023, no proof of service has
8 been filed. On November 29, 2023, the Court entered an Order deeming the *Vasquez* Action
9 complex and staying the discovery and responsive pleading deadline.

10 7. The Included Actions are complex within the meaning of C.C.P. §404 and C.R.C.
11 Rule 3.400. One of the Included Actions has already been ruled to meet the standards for complex
12 cases pursuant to C.R.C. Rule 3.400, and the Included Actions as a whole are surely even more
13 complex, not less. The Included Actions have been brought as class actions, which are inherently
14 complex. C.R.C. Rule 3.400(c)(6). Resolution of the Included Actions will require coordination to
15 conserve judicial resources and ensure consistent results, including with regards to dispositive
16 motions and motions for class certification. *See* C.R.C. Rule 3.400(b)(4). Given the scale of the
17 breach, involving millions of customers, and the sensitivity of the information compromised, there
18 will likely be a large number of witnesses and substantial documentary evidence. *See* C.R.C. Rule
19 3.400(b)(2) & (3). Expert testimony will be required at class certification and trial to resolve
20 various complex issues including regarding the types of data compromised, the vectors of
21 compromise, and the types of security measures that would have been reasonable to implement
22 under the circumstances. *See* C.R.C. Rule 3.400(b)(1). Finally, any consent judgments resolving
23 these cases – which will likely require ongoing injunctive relief to prevent against any further
24 breaches – will require substantial post-judgment supervision. *See* C.R.C. Rule 3.400(b)(5).

25 8. Petitioner relies upon the following facts to show that each Included Action meets
26 the coordination standards specified in C.C.P. §404.1: (1) substantially similar legal issues and
27 factual allegations predominate in the Included Actions; (2) coordination would be more
28 convenient for the parties and their counsel; (3) coordination will promote judicial efficiency by

1 requiring only one judge to become familiar with the legal questions and scientific issues at the
 2 heart of these cases; (4) absent coordination, there is a significant risk of conflicting court rulings;
 3 and (5) coordination will significantly promote settlement of the claims raised in the Included
 4 Actions. Thus, coordination of the Included Actions before a single judge will promote the ends of
 5 justice.

6 9. Petitioner requests coordination of the Included Actions in San Francisco County,
 7 where Defendants are headquartered, and the relevant witnesses will be located. Accordingly,
 8 venue in San Francisco County will be convenient for the parties, witnesses, and counsel.
 9 23andMe is headquartered in San Francisco County. (“Our corporate headquarters was previously
 10 located in Sunnyvale, California. . . . Effective April 1, 2022, we relocated our corporate
 11 headquarters to South San Francisco, California.”).¹ In petitioning the Judicial Panel on
 12 Multidistrict Litigation to transfer and coordinate the actions against it pending in the Northern
 13 District of California, 23andMe specifically argued that proceeding anywhere else would be
 14 prejudicial to 23andMe “given its presence in South San Francisco.” Memorandum of Law in
 15 Support of Motion for Transfer and Consolidation of 23andMe, Inc. Litigation Pursuant to 28
 16 U.S.C. §1407, MDL No. 3098, ECF No. 1-1 at 9 (J.P.M.L. Dec. 21, 2023). The Included Actions
 17 are in their earliest phases and no active litigation has taken place in either of the Included Actions.
 18 The *Vasquez* Action is currently stayed. No party will be prejudiced by a transfer of the *Vasquez*
 19 Action to San Francisco County at this early stage in the litigation.

20 10. For the reasons stated in Paragraph No. 9, Petitioner requests that any hearing of this
 21 Petition also be set at the San Francisco County Superior Court.

22 Dated: January 24, 2024

LEXINGTON LAW GROUP



24 Mark N. Todzo (Bar No. 168389)
 25 Patrick R. Carey (Bar No. 308623)
 26 Meredyth L. Merrow (Bar No. 328337)
 503 Divisadero Street
 San Francisco, CA 94117

27
 28 ¹ See 23andMe Holding Co., Annual Report (Form 10-K) (March 31, 2022),
<https://investors.23andme.com/static-files/536ba9a7-8a85-4b73-8b09-8215451089a0>.

Telephone: (415) 913-7800
Facsimile: (415) 759-4112
mtodzo@lexlawgroup.com

Joseph P. Guglielmo (*pro hac vice* forthcoming)
Carey Alexander (*pro hac vice* forthcoming)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169-1820
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com

Attorneys for Petitioner

Exhibit B

RECEIVED

Judicial Council of California

JAN 24 2024

Grace Dilgura (l.a.)
Coordination Lawyer

1 Mark N. Todzo (Bar No. 168389)
2 **LEXINGTON LAW GROUP**
3 503 Divisadero Street
4 San Francisco, CA 94117
5 Telephone: 415-913-7800
6 Facsimile: 415-759-4112
7 mtodzo@lexlawgroup.com

8 *Attorneys for Petitioner*

9 [Additional Counsel on Signature Page.]

10 **JUDICIAL COUNCIL OF THE STATE OF CALIFORNIA**

11 IN THE MATTER OF THE REQUEST FOR
12 COORDINATION OF THE FOLLOWING
13 ACTIONS:

14 IN THE SUPERIOR COURT FOR THE
15 COUNTY OF SAN FRANCISCO (Case No.
16 CGC-23-610816)

17 MARJORIE MORGENSTERN on Behalf of
18 Herself and All Others Similarly Situated,

19 Plaintiff,

20 v.

21 23ANDME HOLDING CO. and 23ANDME,
22 INC.,

23 Defendants.

24 IN THE SUPERIOR COURT FOR THE
25 COUNTY OF SANTA CLARA (Case No.
26 23CV424996):

27 KATHY VASQUEZ, Individually and on Behalf
28 of All Others Similarly Situated,

Plaintiff,

v.

23ANDME, INC.,

Defendant.

Judicial Counsel Coordination Proceeding
No. **5315**

**DECLARATION OF MARK N.
TODZO IN SUPPORT OF PETITION
FOR COORDINATION**

[Filed concurrently with Petition for
Coordination; MPA ISO Petition for
Coordination; Application for Stay Order]

HEARING REQUESTED

1 I, Mark N. Todzo, declare:

2 1. I am a member in good standing with the California State Bar. I am a partner with
3 the Lexington Law Group, and I represent plaintiff Marjorie Morgenstern (“Petitioner”) in the
4 action captioned as *Morgenstern v. 23andMe Holding Co., et al.* (San Francisco Case No. 23-
5 610816). I have personal knowledge of the matters set forth herein and, if called upon, I could and
6 would competently testify thereto.

7 2. I submit this declaration in support of Petitioner’s Petition for Coordination Pursuant
8 to Code of Civil Procedure (“C.C.P.”) §404. The Petition seeks coordination of the following
9 actions (the “Included Actions”), each of which results from a massive data breach at 23andMe
10 Holding Co. and 23andMe, Inc. (collectively, “23andMe”), which compromised the personal
11 identifiable information (“PII”) and personal genetic and health information (“PGI”) of millions of
12 customers:

- 13 a. *Morgenstern v. 23andMe Holding Co., et al.* (San Francisco Case No. 23-
14 610816) (the “*Morgenstern Action*”); and
- 15 b. *Vasquez v. 23andMe, Inc.*, (Santa Clara Case No. 23CV424996) (the
16 “*Vasquez Action*”).

17 Petitioner anticipates that there may be additional actions filed in the future addressing the
18 23andMe data breach that will need to be treated as add-on cases under C.C.P. §404.4. Besides
19 this, Petitioner is presently aware of no other pending California actions that share a predominating
20 common question of fact or law with the Included Actions such that coordination is required.

21 **The 23andMe Data Breach**

22 1. 23andMe sells direct-to-consumer genetic testing kits to the public. To use
23 23andMe’s services, customers are required to provide a saliva sample that is subjected to single
24 nucleotide polymorphism (“SNP”) genotyping. 23andMe identifies more than half of a million SNPs
25 from each saliva sample, which it uses to identify traits related to a person’s ancestry, wellness, health
26 predispositions (including genetic health risks), and carrier status for inherited conditions.

2. 23andMe claims to have more than 14 million customers.¹ According to 23andMe: “We receive and store a large volume of [personally identifiable information (“PII”) and personal genetic and health information (“PGI”)], and other data relating to our customers and patients. . . .”²

3. On October 1, 2023, a hacker posted online a claim to have 23andMe users’ profile information. On October 6, 2023, 23andMe confirmed that “customer profile information” had been accessed “without the account users’ authorization,” and that a hacker had “obtained information from certain accounts, including information about users’ DNA Relatives profiles . . .” (the “Data Breach”).³ 23andMe has since stated that the information accessed by the hacker “generally included ancestry information, and, for a subset of those accounts, health-related information based upon the user’s genetics.”⁴ Posts on the dark web have purported to sell access to tens of millions of pieces of raw data exfiltrated from 23andMe.

4. Petitioner filed the *Morgenstern* Action on December 4, 2023, in San Francisco County Superior Court. The *Morgenstern* Action asserts eight claims for relief against 23andMe, including for violations of California’s Unfair Competition Law, Cal. Bus. & Prof. Code §17200, California’s Consumer Privacy Act (“CCPA”), Cal. Civ. Code §17983.100, *et seq.*, and California’s Genetic Information Privacy Act (“GIPA”), Cal. Civ. Code §56.18, as well as claims for relief under the common law. Petitioner is represented by the Lexington Law Group, a San Francisco-based firm and by Scott+Scott Attorneys at Law LLP, an international class action firm with its primary office in New York. A true and correct copy of Petitioner’s Complaint in the *Morgenstern* Action is attached hereto as **Exhibit 1**.

5. Petitioner has duly served the operative Complaint and a summons on 23andMe. Executed proofs of service were filed on January 9, 2024. On December 15, 2023, Petitioner filed

¹ *23andMe for Healthcare Professionals*, 23ANDME (Nov. 3, 2023), <https://medical.23andme.com> [<https://web.archive.org/web/20231030132819/https://medical.23andme.com/>]

² 23andMe Holding Co., Annual Report (Form 10-K) at 72 (March 31, 2022), <https://investors.23andme.com/static-files/536ba9a7-8a85-4b73-8b09-8215451089a0>.

³ *Addressing Data Security Concerns*, 23ANDME (Oct 6, 2023; updated Dec. 5, 2023), <https://blog.23andme.com/articles/addressing-data-security-concerns> [<https://web.archive.org/web/20231007110808/https://blog.23andme.com/articles/addressing-data-security-concerns>].

⁴ 23andMe Holding Co., Form 8-K/A, Am. 1 (Oct. 10, 2023).

1 a Notice of Related Cases indicating the Morgenstern Action's relation to cases pending in Federal
2 Court in the Northern District of California. On December 19, 2023, Petitioner filed an application
3 to designate the Morgenstern Action as complex, which remains pending. An initial case
4 management conference has been set for May 8, 2024.

5 6. The *Vasquez* Action was filed in Santa Clara Superior Court on October 31, 2023.
6 The *Vasquez* Action asserts seven claims for relief, most of which are also asserted in the
7 *Morgenstern* Action. A true and correct copy of the Complaint from the *Vasquez* Action is
8 attached hereto as **Exhibit 2**.

9 7. In the *Vasquez* Action, it does not appear that a proof of service of the summons has
10 been filed on the docket. On November 29, 2023, the Court entered an Order deeming the *Vasquez*
11 Action complex. A copy of the Order deeming the *Vasquez* Action complex is attached as **Exhibit**
12 **3**.

13 8. Discovery and the responsive pleading deadlines in the *Vasquez* Action have been
14 stayed. An initial case management conference is set for March 14, 2024.

15
16 I declare under penalty of perjury under the laws of the State of California that the
17 foregoing is true and correct, and that this declaration is executed on this 24th day of January,
18 2024, at San Francisco, California.

19
20 

21 Mark N. Todzo

EXHIBIT 1

1 Mark N. Todzo (Bar No. 168389)

2 **LEXINGTON LAW GROUP**

3 503 Divisadero Street

4 San Francisco, CA 94117

5 Telephone: 415-913-7800

6 Facsimile: 415-759-4112

7 mtodzo@lexlawgroup.com

8 *Attorneys for Plaintiff*

9 [Additional Counsel on Signature Page.]

ELECTRONICALLY

FILED

Superior Court of California,
County of San Francisco

12/04/2023

Clerk of the Court

BY: ERNALYN BURA

Deputy Clerk

10 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**

11 **COUNTY OF SAN FRANCISCO**

12 MARJORIE MORGENSTERN on Behalf of
13 Herself and All Others Similarly Situated,

14 Plaintiff,

15 v.

16 23ANDME HOLDING CO. and 23ANDME,
17 INC.,

18 Defendants.

No.

CLASS ACTION

CGC-23-610816

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff Marjorie Morgenstern (“Plaintiff”), on behalf of herself and all others similarly
 2 situated, files this Complaint against Defendants 23andMe Holding Co. and 23andMe, Inc.
 3 (“23andMe” or “Defendant”). The following allegations are based upon Plaintiff’s personal
 4 knowledge with respect to herself and her own acts and upon information and belief as to all other
 5 matters following her and her counsel’s investigation.

6 INTRODUCTION

7 1. 23andMe hails itself as the “pioneer[]” of direct-to-consumer genetic testing and
 8 boasts that it has the “premier database of genetic and phenotypic information crowdsourced from
 9 its millions of customers” capable of providing “personalized information about [consumers’]
 10 genetic health risks, ancestry, and traits.”¹

11 2. 23andMe knowingly collects and stores troves of personally identifiable
 12 information (“PII”) and personal genetic and health information (“PGI”) and has a corresponding
 13 duty to implement and maintain reasonable security measures to keep that data secure. PII and
 14 PGI is property owned by Plaintiff and members of the Class that was shared with 23andMe for a
 15 limited purpose with the understanding that 23andMe would implement and maintain reasonable
 16 data security measures adequate to protect PII and PGI.

17 3. “[G]enetic information is inherently identifiable. . . .”² Unlike other types of
 18 personal information like financial information or Social Security Numbers, genetic information
 19 is immutable. “Once an individual’s genetic data is breached it can no longer be protected.”³
 20 Because genetic data is tied “intrinsically to our identity. . . genetic data breaches can have long-
 21
 22
 23

24 ¹ 23andMe Holding Co., Annual Report (Form 10-K) (March 31, 2022),
 25 <https://investors.23andme.com/static-files/536ba9a7-8a85-4b73-8b09-8215451089a0>.

26 ² Emily Christofides & Kieran O’Doherty, *Company Disclosure and Consumer Perceptions*
 27 *of the Privacy Implications of Direct-to-Consumer Genetic Testing*, NEW GENETICS AND SOCIETY
 35:2, 101-123 (2016).

28 ³ Sawaya, Sterling and Kenneally, Erin E. and Nelson, Demetrius and Schumacher, Garrett
 J., *Artificial Intelligence and the Weaponization of Genetic Data* at 13, SSRN (April 24, 2020).

1 lasting consequences and must be considered distinct from other types of data breaches.”⁴ Genetic
 2 data also identifies immutable relationships with others. With the genetic data of just 2% of a
 3 given population, researchers can “provide a third cousin match to nearly any person.”⁵

4 4. On October 6, 2023, 23andMe confirmed that “customer profile information” had
 5 been accessed “without the account users’ authorization,” and that a hacker had “obtained
 6 information from certain accounts, including information about users’ DNA Relatives profiles . . .”
 7 (the “Data Breach”).⁶

8 5. The PII and PGI compromised in the Data Breach has already been offered for sale
 9 on the dark web.

10 6. As a direct and proximate result of 23andMe’s failure to implement and maintain
 11 reasonable data security measures, Plaintiff and members of the Class have lost the ability to
 12 control the use and dissemination of their PII and PGI.

13 **PARTIES**

14 7. Plaintiff Marjorie Morgenstern is a citizen and resident of California.

15 8. Defendant 23andMe Holding Co. is a Delaware corporation with its headquarters
 16 and principal place of business located at 349 Oyster Point Blvd., South San Francisco, California
 17 94080.

18 9. Defendant 23andMe, Inc. is a Delaware corporation with its headquarters and
 19 principal place of business located at 223 N. Mathilda Ave., Sunnyvale, California 94086.

22
 23 ⁴ Sawaya, Sterling and Kenneally, Erin E. and Nelson, Demetrius and Schumacher, Garrett
 J., *Artificial Intelligence and the Weaponization of Genetic Data* at 13, SSRN (April 24, 2020).

24 ⁵ Yaniv Erlich, Tal Shor, Itsik Pe’er, Shai Carmi, *Identity Inference of Genomic Data using*
 25 *Long-Range Familial Searches*, Vol. 362 *SCIENCE* 690 (Oct. 11 2018) (“[W]e predict that with a
 26 database size of ~3 million US individuals of European descent (2% of the adults of this
 population), over 99% of the people of this ethnicity would have at least a single 3rd cousin match
 and over 65% are expected to have at least one 2nd cousin match.”).

27 ⁶ 23andMe, Addressing Data Security Concerns (Oct 6, 2023), [https://blog.23andme.com/](https://blog.23andme.com/articles/addressing-data-security-concerns)
 28 [\[https://web.archive.org/web/20231007110808/](https://web.archive.org/web/20231007110808/https://blog.23andme.com/articles/addressing-data-security-concerns)
[https://blog.23andme.com/articles/addressing-data-security-concerns\]](https://blog.23andme.com/articles/addressing-data-security-concerns).

VENUE

10. Venue is proper in this Court pursuant to California Code of Civil Procedure §395 because 23andMe resides in San Francisco County at the commencement of this action.⁷

JURISDICTION

11. This Court has subject-matter jurisdiction over this action pursuant to the California Constitution, Article VI § 10.

12. This Court has personal jurisdiction over Defendants pursuant to California Code of Civil Procedure §410.10 because 23andMe is headquartered in California, its principal place of business is in California, and it regularly conducts business in California.

FACTUAL BACKGROUND

A. 23andMe

13. 23andMe sells direct-to-consumer genetic testing kits to the public. To use 23andMe’s services, customers are required to provide a saliva sample that is subjected to single nucleotide polymorphism (“SNP”) genotyping. 23andMe identifies more than half a million SNPs from each saliva sample, which it uses to identify traits related to a person’s ancestry, wellness, health predispositions (including genetic health risks), and carrier status for inherited conditions.

14. 23andMe claims to have more than 14 million customers.⁸ According to 23andMe: “We receive and store a large volume of [PII], [PGI], and other data relating to our customers and patients. . . .”⁹

15. The PII and PGI that 23andMe collects undoubtedly has value. 23andMe claims that “insights” from customers’ PII and PGI “may highlight opportunities to develop a drug to treat

⁷ 23andMe Holding Co., Annual Report (Form 10-K) (March 31, 2022), <https://investors.23andme.com/static-files/536ba9a7-8a85-4b73-8b09-8215451089a0> (“Our corporate headquarters was previously located in Sunnyvale, California. . . . Effective April 1, 2022, we relocated our corporate headquarters to South San Francisco, California.”).

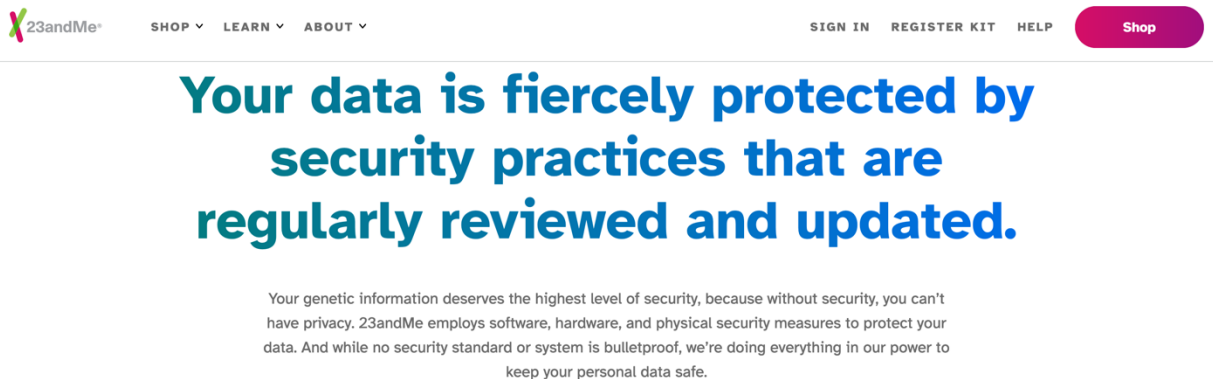
⁸ 23andMe for Medical Professionals, (Nov. 3, 2023), <https://medical.23andme.com/> [<https://web.archive.org/web/20231030132819/https://medical.23andme.com/>]

⁹ Form 10-K, *supra* n.7 at 72.

or cure a specific disease, and also provide information that customers can use to enhance their medical care and treatment.”¹⁰

16. Plaintiff and Class members reasonably expected that 23andMe would implement and maintain security measures adequate to protect their PII and PGI.

17. 23andMe tells customers that their “genetic information deserves the highest level of security, *because without security, you can’t have privacy*.”¹¹ [Emphasis added.]




Source: 23andMe¹²


18. 23andMe acknowledged that using its services required customers to “entrust us with important personal information.”

¹⁰ *Id.* at 10.

¹¹ Privacy and Data Protection, (Nov. 6, 2023), 23andMe, <https://www.23andme.com/privacy/> [https://web.archive.org/web/20231001063147/; <https://www.23andme.com/privacy/>].

¹² *Id.*

1  SHOP ▾ LEARN ▾ ABOUT ▾

2 

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

SIGN IN REGISTER KIT HELP [Shop](#)

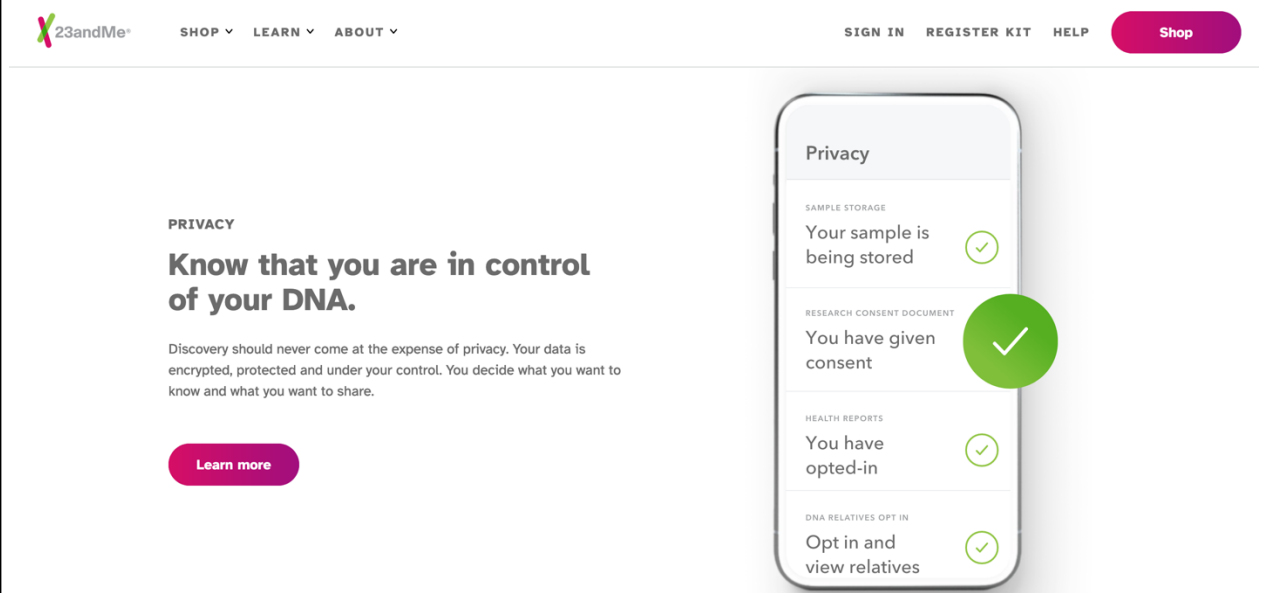
Your privacy comes first.

When you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected.

Source: 23andMe¹³

¹³ *Id.*

19. 23andMe promises customers that they are “in control” of their DNA, stating: “You decide what you want to know and what you want to share.”¹⁴



Source: 23andMe¹⁵

B. The Data Breach

20. On October 1, 2023, a hacker going by the handle “Golem”¹⁶ posted a link to what the hacker called: “The most valuable data you’ll ever see.”¹⁷ The link, which was posted on a “popular forum where stolen data is traded and sold,”¹⁸ contained a sample of nearly “20 million pieces of data” the hacker claimed to have exfiltrated from 23andMe. The data included “genomic

¹⁴ *Id.*

¹⁵ *Id.*

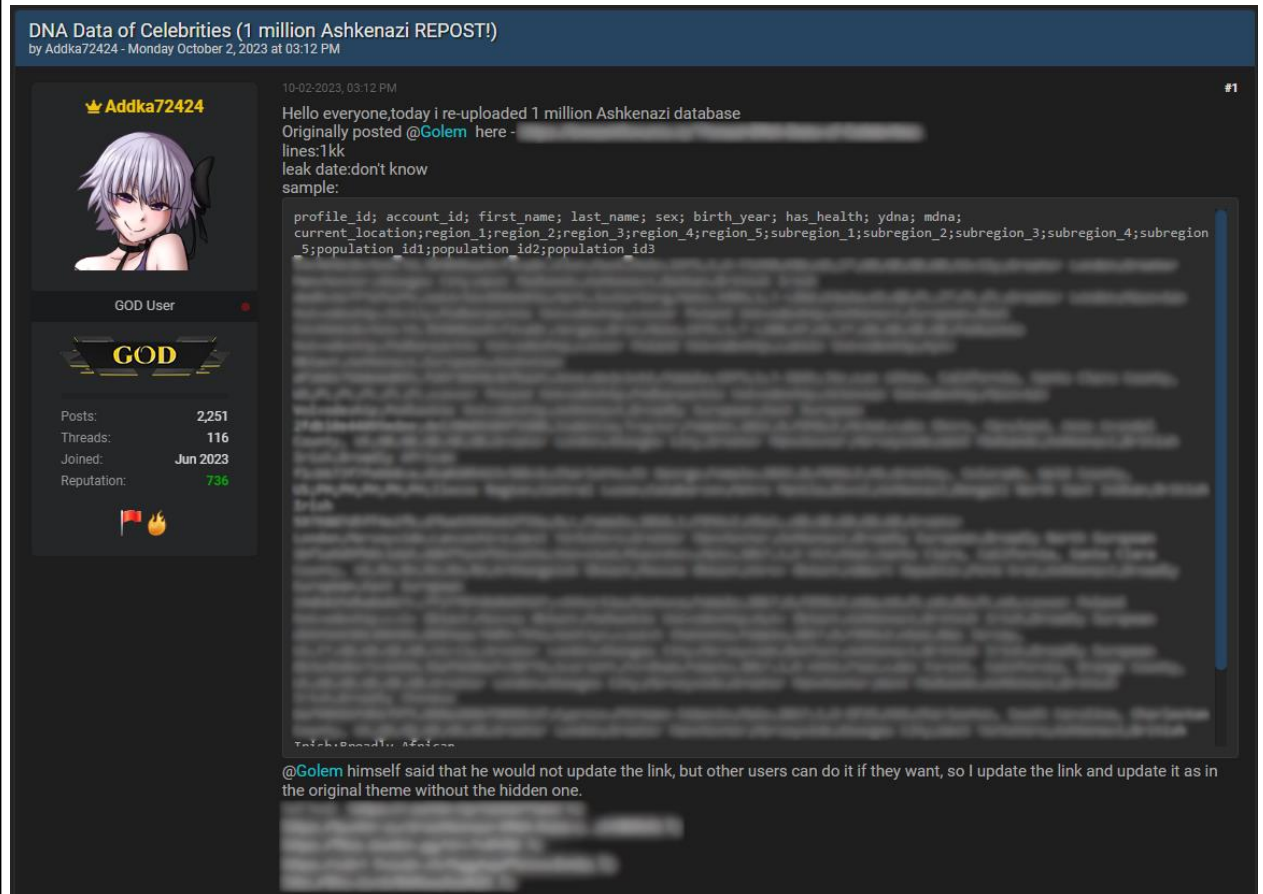
¹⁶ See also *Oxford English Dictionary*, s.v. “golem, n., sense 1,” July 2023, <https://doi.org/10.1093/OED/4113804198> (“[T]he golem was said to have been created by Rabbi Löw of Prague (d. 1609) in order to protect the city’s Jewish population from pogroms. However, the golem began to act independently of its master and so the rabbi returned it to dust.”).

¹⁷ AJ Vicens, *DNA testing service 23andMe investigating theft of user data*, CYBERSCOOP (Oct. 5, 2023), <https://cyberscoop.com/23andme-user-data-theft/>; see also *DNA Data of Celebrities*, BREACHFORUMS (Oct. 1, 2023), <https://breachforums.is/Thread-DNA-Data-of-Celebrities> [<https://webcache.googleusercontent.com/search?q=cache:cOVRhJGEU5kJ:https://breachforums.is/Thread-DNA-Data-of-Celebrities>].

¹⁸ Vicens, *supra* n.17.

ancestry data owned by 1 million Ashkenazi,” with “an extra 1 million Ashkenazi data available.”¹⁹ The hacker offered to sell the “[r]aw data” for a “fee” of “\$5 each.”²⁰

21. On October 2, 2023, the data was reposted along with a sample of the data compromised purportedly associated with 1 million individuals of Ashkenazi descent and 100,000 individuals of Chinese descent.



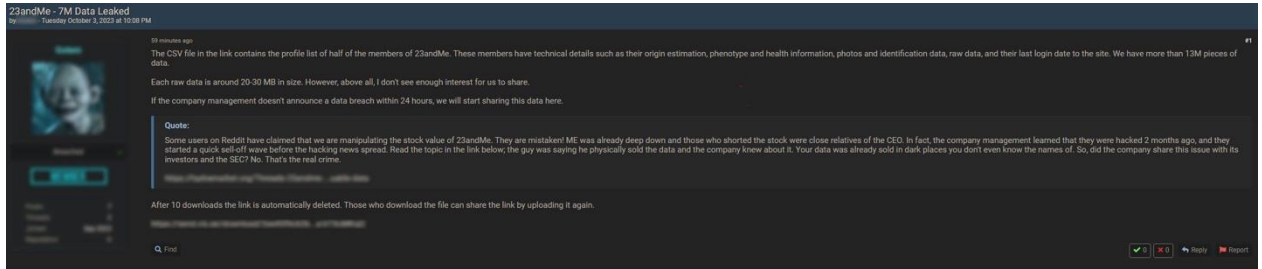
Source: Bleeping Computer²¹

¹⁹ *DNA Data of Celebrities*, BREACHFORUMS (Oct. 1, 2023), <https://breachforums.is/Thread-DNA-Data-of-Celebrities> [https://webcache.googleusercontent.com/search?q=cache:cOVRhJGEU5kJ: https://breachforums.is/Thread-DNA-Data-of-Celebrities].

²⁰ *Id.*

²¹ Bill Toulas, *Genetics firm 23andMe says user data stolen in credential stuffing attack*, BLEEPING COMPUTER (Oct. 6, 2023 11:48 AM), <https://www.bleepingcomputer.com/news/security/genetics-firm-23andme-says-user-data-stolen-in-credential-stuffing-attack/> [https://web.archive.org/web/20231006172221/https://www.bleepingcomputer.com/news/security/genetics-firm-23andme-says-user-data-stolen-in-credential-stuffing-attack/]; *DNA Data of Celebrities* (1 million Ashkenazi REPOST!), BreachForums (Oct. 2, 2023),

22. On October 3, 2023, the hacker again posted, claiming that the compromised data contained “technical details such as their origin estimation, phenotype and health information, photos and identification data, [and] raw data,” among other data points. The hacker added that the Data Breach compromised “13M pieces of data,” and that “[e]ach raw data [file] is around 20-30 MB in size.”



Source: Recorded Future News²²

23. On October 4, 2023, under the heading “23andMe – Genetic Data For Sale,” the hacker posted again, claiming to have “tailored ethnic groupings, individualized data sets, pinpointed origin estimations, haplogroup details, phenotype information, photographs, links to

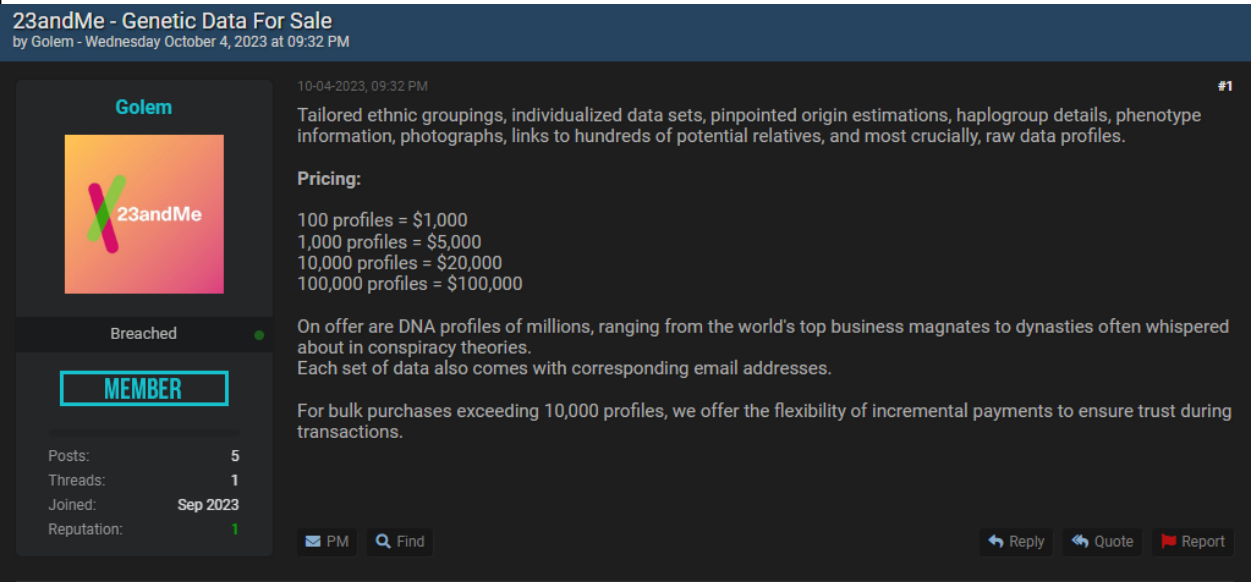
<https://breachforums.is/Thread-DNA-Data-of-Celebrities-1-million-Ashkenazi-REPOST> [<https://webcache.googleusercontent.com/search?q=cache:Tk1as80qBkYJ:https://breachforums.is/Thread-DNA-Data-of-Celebrities-1-million-Ashkenazi-REPOST>]; DNA Data of Celebrities (100,000 Chinese), BreachForums (Oct. 2, 2023), <https://breachforums.is/Thread-DNA-Data-of-Celebrities-100-000-Chinese> [<https://webcache.googleusercontent.com/search?q=cache:BHqAR1agkKoJ:https://breachforums.is/Thread-DNA-Data-of-Celebrities-100-000-Chinese>].

²² Jonathan Greig, *23andMe scraping incident leaked data on 1.3 million users of Ashkenazi and Chinese descent*, RECORDED FUTURE NEWS (Oct. 6, 2023), <https://therecord.media/scraping-incident-genetic-testing-site> [<https://web.archive.org/web/20231006200925/https://therecord.media/scraping-incident-genetic-testing-site>].

hundreds of potential relatives, and most crucially, raw data profiles.”²³ The hacker offered the data for sale in 100, 1,000, 10,000 and 100,000-profile batches.²⁴

23andMe - Genetic Data For Sale
by Golem - Wednesday October 4, 2023 at 09:32 PM

10-04-2023, 09:32 PM #1



Tailored ethnic groupings, individualized data sets, pinpointed origin estimations, haplogroup details, phenotype information, photographs, links to hundreds of potential relatives, and most crucially, raw data profiles.

Pricing:

100 profiles =	\$1,000
1,000 profiles =	\$5,000
10,000 profiles =	\$20,000
100,000 profiles =	\$100,000

On offer are DNA profiles of millions, ranging from the world's top business magnates to dynasties often whispered about in conspiracy theories. Each set of data also comes with corresponding email addresses.

For bulk purchases exceeding 10,000 profiles, we offer the flexibility of incremental payments to ensure trust during transactions.

Posts: 5
Threads: 1
Joined: Sep 2023
Reputation: 1

PM Find Reply Quote Report

Source: Bleeping Computer²⁵

24. On October 6, 2023, 23andMe confirmed that PII and PGI had been compromised in the Data Breach, stating in a post on its website:

We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorization.

[. . .]

We believe that the threat actor may have . . . accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles, to the extent a user opted into that service.²⁶

²³ AJ Vicens, *DNA testing service 23andMe investigating theft of user data*, CYBERSCOOP (Oct. 5, 2023), <https://cyberscoop.com/23andme-user-data-theft/>.

²⁴ *Id.*

²⁵ Toulas, *supra* n.21.

²⁶ Addressing Data Security Concerns (Oct. 6, 2023), <https://blog.23andme.com/articles/addressing-data-security-concerns> [<https://web.archive.org/web/20231007110808/https://blog.23andme.com/articles/addressing-data-security-concerns>].

1 25. On October 9, 2023, 23andMe updated its post to state:

2 We are reaching out to our customers to provide an update on the
3 investigation and to encourage them to take additional actions to
4 keep their account and password secure. Out of caution, we are
5 requiring that all customers reset their passwords and are
6 encouraging the use of multi-factor authentication (MFA).

7 If we learn that a customer's data has been accessed without their
8 authorization, we will notify them directly with more information.²⁷

9 26. 23andMe identifies the specific data elements potentially available through the
10 DNA Relatives profiles, including display name, recent login activity, genetic gender, predicted
11 relationship and percentage of DNA shared with potential family members, ancestry composition,
12 maternal and paternal haplogroups, Neanderthal ancestry results, matching DNA segments, birth
13 location, current location, profile picture, birth year, family trees, and any other family information
14 entrusted to 23andMe.²⁸

15 27. 23andMe blamed its customers for the breach, claiming that it believed "threat
16 actors were able to access certain accounts" where "usernames and passwords that were used on
17 23andMe.com were the same as those used on other websites that have been previously hacked."²⁹

18 28. 23andMe's response was merely "encouraging" users to enable multi-factor
19 authentication.

20 29. Multi-factor authentication works by requiring users to provide more than a mere
21 password to login to a website; users must instead provide a second factor of authentication,
22 usually a code generated by an application or sent via text, to login, ensuring that the individual
23 presenting the password is the same individual with access to the device presenting the
24 authentication code.

25 ²⁷ *Id.*

26 ²⁸ DNA Relatives Privacy and Display Settings, [https://customercare.23andme.com/hc/en-](https://customercare.23andme.com/hc/en-us/articles/18262768896023)
27 us/articles/18262768896023 [https://web.archive.org/web/20231015073225/
28 <https://customercare.23andme.com/hc/en-us/articles/18262768896023>].

²⁹ Addressing Data Security Concerns, *supra* n.26.

30. If 23andMe's belief as to the cause of the Data Breach were correct, requiring users to enable multi-factor authentication could have prevented the Data Breach.

31. Requiring users to enable multi-factor authentication is considered by security researchers and industry professionals to be "[b]asic security hygiene" that "can protect against 98% of attacks."³⁰ That's why, according to Microsoft, "almost all online services - banks, social media, shopping" use multi-factor authentication to secure accounts.³¹ Similarly, according to Google: "One of the best ways to protect your account from a breached or bad password is by having a second form of verification in place – another way for your account to confirm it is really you logging in."³² That's why in 2021, Google began "automatically enrolling" users in multi-factor authentication.³³

32. To this day, 23andMe has not required its users to enroll in multi-factor authentication.

C. Plaintiff's PII and PGI Was Compromised in the Data Breach

33. Plaintiff paid approximately \$100 to purchase a 23andMe testing kit and provided her PII and PGI to 23andMe in approximately 2015.

34. On October 12, 2023, 23andMe provided notice of the Data Breach to Plaintiff and stated: "If we learn that your data has been accessed without your authorization, we will contact you separately with more information."

35. On October 24, 2023, 23andMe provided a supplemental notice to Plaintiff that stated in relevant part: "After further review, we have identified your DNA Relatives profile as

³⁰ Andrea Fisher, *Is MFA the Vegetable of Cybersecurity?*, DARK READING (Dec. 1, 2022), <https://www.darkreading.com/microsoft/is-mfa-the-vegetable-of-cybersecurity>.

³¹ *What is: Multifactor Authentication*, <https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661> ("Compromised passwords are one of the most common ways that bad guys can get at your data, your identity, or your money. Using multifactor authentication is one of the easiest ways to make it a lot harder for them.").

³² Mark Risher, *A simpler and safer future — without passwords*, GOOGLE (May 6, 2021), <https://blog.google/technology/safety-security/a-simpler-and-safer-future-without-passwords/>.

³³ *Id.*

one that was impacted in this incident. Specifically, there was unauthorized access to one or more 23andMe accounts that were connected to you through DNA Relatives. As a result, the DNA Relatives profile information you provided in this feature was exposed to the threat actor.”

36. Plaintiff would not have purchased a 23andMe testing kit or provided her PII and PGI to 23andMe if she had known that 23andMe had failed to implement and maintain reasonable security measures adequate to secure her PII and PGI.

37. As a direct and proximate result of 23andMe’s conduct, Plaintiff has lost the ability to control the use and dissemination of her PII and PGI.

D. 23andMe Specifically Knew of the Risk of the Data Breach

38. The risk of the Data Breach was eminently foreseeable to 23andMe. In its Form 10-K statement, 23andMe specifically acknowledged and warned of the risk of a data breach that could compromise PII and PGI:

Increased global IT security threats and more sophisticated and targeted computer crime pose a risk to the security of our systems and networks and the confidentiality, availability, and integrity of our data. There have been several recent, highly publicized cases in which organizations of various types and sizes have reported the unauthorized disclosure of customer or other confidential information, as well as cyberattacks involving the dissemination, theft, and destruction of corporate information, intellectual property, cash, or other valuable assets. There have also been several highly publicized cases in which hackers have requested “ransom” payments in exchange for not disclosing customer or other confidential information or for not disabling the target company’s computer or other systems. A security breach or privacy violation that leads to disclosure or unauthorized use or modification of, or that prevents access to or otherwise impacts the confidentiality, security, or integrity of, sensitive, confidential, or proprietary information we or our third-party service providers maintain or otherwise process, could compel us to comply with breach notification laws, and cause us to incur significant costs for remediation, fines, penalties, notification to individuals and governmental authorities, implementation of measures intended to repair or replace systems or technology, and to prevent future occurrences, potential increases in insurance premiums, and forensic security audits or investigations. Additionally, a security compromise of our information systems or of those of businesses with whom we interact that results in confidential information being accessed by unauthorized or improper persons could harm our reputation and expose us to customer and patient attrition, and

claims brought by our customers, patients, or others for breaching contractual confidentiality and security provisions or data protection laws. Monetary damages imposed on us could be significant and not covered by our liability insurance.³⁴

39. 23andMe bluntly acknowledged that its customers, including Plaintiff and Class members, considered it material that 23andMe had implemented and maintained reasonable data security measures adequate to protect PII and PGI, stating that “[e]ven the *perception* that the privacy of personal information is not satisfactorily protected or does not meet regulatory requirements could inhibit sales of our solutions. . . .” [Emphasis added.]³⁵

40. The risks of data breaches has long been well-known. In 2015, IBM’s CEO warned: “Cyber crime is the greatest threat to every company in the world.”³⁶ The number of U.S. data breaches surpassed 1,000 in 2016, a 40% increase in the number of data breaches from the previous year.³⁷ In 2017, a new record high of 1,579 breaches were reported representing a 44.7% increase.³⁸ That upward trend continues.

41. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.³⁹

³⁴ Form 10-K, *supra* n.7.

³⁵ *Id.*

³⁶ Sofia Said Birch, *IBM’s CEO on hackers: “Cyber crime is the greatest threat to every company in the world,”* IBM NORDIC BLOG (Nov. 15, 2015), <https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/>.

³⁷ *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, CISION PR NEWSWIRE (Jan. 19, 2017), <https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html>.

³⁸ *2017 Annual Data Breach Year-End Review*, IDENTITY THEFT RES. CTR., <https://www.idtheftcenter.org/wp-content/uploads/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf>.

³⁹ *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf.

42. A robust black market exists in which criminals openly post stolen PII, PGI, and related information on the dark web.

43. PII and PGI have tremendous value. According to the FTC, if hackers get access to personally identifiable information, they will use it.⁴⁰ While credit card information and associated PII can sell for as little as \$1-\$2 on the black market, health information alone can sell for as much as \$363.⁴¹ Because of its immutability, PGI is worth even more.

44. The Federal Trade Commission Act (“FTCA”) (15 U.S.C. §45) prohibited 23andMe from engaging in “unfair or deceptive acts or practices in or affecting commerce.” According to the FTC, a company’s failure to implement or maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTCA.

45. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁴²

46. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.⁴³ The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

⁴⁰ Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM’N (May 24, 2017), <https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

⁴¹ See *Data Breaches: In the Healthcare Sector*, CTR. FOR INTERNET SEC., <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/> (last visited Nov. 7, 2023).

⁴² *Start With Security: A Guide for Business*, FED. TRADE COMM’N, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

⁴³ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION: <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last visited Nov. 7, 2023).

1 understand their network's vulnerabilities; and implement policies to correct any security
2 problems.

3 47. The FTC further recommends that companies not maintain PII or PGI longer than
4 is needed; limit access to private data; require complex passwords to be used on networks; use
5 industry-tested methods for security; and monitor for suspicious activity on the network.⁴⁴

6 48. The FTC has brought enforcement actions against businesses for failing to
7 adequately and reasonably protect customer data, treating the failure to employ reasonable and
8 appropriate measures to protect against unauthorized access to confidential consumer data as an
9 unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. §45. Orders resulting from
10 these actions further clarify the measures businesses must take to meet their data security
11 obligations.

12 49. 23andMe failed to implement or maintain reasonable data security measures
13 adequate to protect PII and PGI. 23andMe's failure constitutes an unfair act or practice prohibited
14 by Section 5 of the FTCA, 15 U.S.C. §45.

15 **CLASS ACTION ALLEGATIONS**

16 50. Plaintiff brings this class action on behalf of herself and on behalf of all others
17 similarly situated pursuant to California Code of Civil Procedure § 382.

18 51. Plaintiff seeks certification of a Class currently defined⁴⁵ as follows:

19 All citizens of the State of California whose PII and PGI were
20 compromised in the data breach of 23andMe's systems.

21 52. Excluded from the Class are: Defendants and its subsidiaries and affiliates; all
22 employees of Defendants; all persons who make a timely election to be excluded from the Class;
23 and the judge to whom this case is assigned, including his/her immediate family and court staff.

24 53. **Numerosity:** The Class is so numerous that joinder of all members is impracticable.
25 The hacker associated with the Data Breach claims to have data associated with millions of
26

27 ^{44.} *Id.*

28 ⁴⁵ Plaintiff reserve the right to amend the definition of the proposed Class.

1 individuals whose PII and PGI was compromised. In connection with providing notice of the Data
 2 Breach, 23andMe has confirmed that it can identify individuals whose data was accessed without
 3 their authorization.

4 54. **Commonality and Predominance:** This action involves common questions of law
 5 and fact, which predominate over any questions affecting individual Class members, including,
 6 without limitation:

7 A. whether 23andMe engaged in the misconduct alleged;

8 B. whether 23andMe implemented and maintained data security measures that
 9 were inadequate to protect Plaintiff and Class members' PII and PGI;

10 C. whether 23andMe owed a duty to Plaintiff and Class members and whether
 11 23andMe breached that duty;

12 D. whether 23andMe engaged in unfair or unlawful acts and practices;

13 E. whether Plaintiff and Class members were injured and suffered damages as a
 14 result of 23andMe's conduct; and

15 F. whether Plaintiff and Class members are entitled to relief and the measure of
 16 such relief.

17 55. **Typicality:** Plaintiff had her PII and PGI compromised in the Data Breach.
 18 Plaintiff's claims are typical of the other Class members' claims because, among other things, all
 19 Class members were comparably injured through Defendant's conduct and Plaintiff and each Class
 20 member would assert claims based on the same legal theories.

21 56. **Adequacy:** Plaintiff is an adequate Class representative because she is a member
 22 of the Class she seeks to represent and her interests do not conflict with the interests of the other
 23 members of the Class that she seeks to represent. Plaintiff is committed to pursuing this matter
 24 for the Class with the Class's collective best interests in mind. Plaintiff has retained counsel
 25 competent and experienced in complex class action litigation of this type, and Plaintiff intends to
 26 prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the
 27 Class's interests.
 28

57. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against 23andMe, so it would be impracticable for members of the Class to individually seek redress for 23andMe's conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

58. **Injunctive and Declaratory Relief:** 23andMe, through its uniform conduct, acted or refused to act on grounds generally applicable to each Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Unless a Class-wide injunction is issued, Plaintiff and Class members remain at risk that Defendant will continue to fail to properly secure their PII and PGI, potentially resulting in another data breach.

FIRST CLAIM FOR RELIEF
Negligence

59. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

60. Plaintiff brings this claim on behalf of herself and the Class.

61. 23andMe required Plaintiff and members of the Class to submit PII and PGI to use 23andMe's services.

62. 23andMe knew or should have known of the risks inherent in collecting and storing Plaintiff and Class members' PII and PGI.

63. 23andMe owed a duty of care to Plaintiff and Class members who entrusted their PII and PGI to 23andMe.

64. A special relationship exists between 23andMe and Plaintiff and members of the Class because Plaintiff and members of the Class entrusted their PII and PGI to 23andMe.

65. 23andMe breached its duty of care to Plaintiff and Class members by failing to implement or maintain reasonable security measures adequate to protect Plaintiff and Class members' PII and PGI.

66. As a direct and proximate result of 23andMe's negligent conduct, Plaintiff and members of the Class have been injured.

67. The injuries suffered by Plaintiff and members of the Class were the reasonably foreseeable result of 23andMe's breach of its duty of care to Plaintiff and Class members.

68. Plaintiff and members of the Class are entitled to damages and other relief as this Court considers necessary and proper.

SECOND CLAIM FOR RELIEF

Negligence Per Se

69. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

70. Plaintiff brings this claim on behalf of herself and the Class.

71. 23andMe required Plaintiff and members of the Class to submit PII and PGI to use 23andMe's services.

72. 23andMe knew or should have known of the risks inherent in collecting and storing Plaintiff and Class members' PII and PGI.

73. 23andMe owed a duty of care to Plaintiff and Class members who entrusted their PII and PGI to 23andMe.

74. Pursuant to the FTC Act, 15 U.S.C. §45(a)(1), California's Consumer Privacy Act, Cal. Civ. Code §1798.100 (Deering) Cal. Civ. Code §1798.150, and California's Genetic Information Privacy Act, Cal. Civ. Code §56.18 (Deering), 23andMe had a duty to implement and maintain reasonable security measures adequate to protect Plaintiff's and Class members' PII and PGI.

75. 23andMe breached its duty of care to Plaintiff and Class members by failing to implement or maintain reasonable security measures adequate to protect Plaintiff and Class members' PII and PGI in violation of the FTC Act, California's Consumer Privacy Act, and California's Genetic Information Privacy Act.

76. As a direct and proximate result of 23andMe's negligent conduct, Plaintiff and members of the Class have been injured.

77. The injuries suffered by Plaintiff and members of the Class were the reasonably foreseeable result of 23andMe's breach of its duty of care to Plaintiff and Class members.

78. Plaintiff and members of the Class are entitled to damages and other relief as this Court considers necessary and proper.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract

79. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

80. Plaintiff brings this claim on behalf of herself and the Class.

81. 23andMe required Plaintiff and members of the Class to pay 23andMe and to submit PII and PGI to use 23andMe's services.

82. 23andMe impliedly agreed to implement and maintain reasonable data security measures that complied with industry standards and was adequate to protect PII and PGI in exchange for receiving Plaintiff and Class members' PII, PGI, and payments.

83. Plaintiff and members of the Class paid 23andMe and submitted their PII and PGI to 23andMe.

84. Plaintiff and members of the Class would not have paid 23andMe or submitted their PII and PGI to 23andMe unless 23andMe agreed to implement and maintain reasonable data security measures that complied with industry standards and was adequate to protect PII and PGI.

85. 23andMe breached its agreements with Plaintiff and members of the Class by implementing and maintaining unreasonable data security measures that were inadequate to protect PII and PGI or prevent the Data Breach.

1 97. Plaintiff and members of the Class are entitled to damages and other relief as this
2 Court considers necessary and proper.

3 **FIFTH CLAIM FOR RELIEF**
4 **Conversion**

5 98. Plaintiff incorporates and realleges each and every allegation contained above as if
6 fully set forth herein.

7 99. Plaintiff brings this claim on behalf of herself and the Class.

8 100. Plaintiff and members of the Class have an interest in maintaining their right to
9 control the use and dissemination of their PII and PGI.

10 101. 23andMe has exercised dominion over Plaintiff and Class members' PII and PGI
11 by disclosing it without their permission.

12 102. As a direct and proximate result of 23andMe's conduct, Plaintiff and members of
13 the Class have lost the exclusive right to control the use and dissemination of their PII and PGI.

14 103. Plaintiff and members of the Class are entitled to damages and other relief as this
15 Court considers necessary and proper.

16 **SIXTH CLAIM FOR RELIEF**
17 **Violation of The California Unfair Competition Law,**
18 **Cal. Bus. & Prof. Code §17200 Based On "Unfair" and/or "Unlawful" Acts and Practices**

19 104. Plaintiff incorporates and realleges each and every allegation contained above as if
20 fully set forth herein.

21 105. Plaintiff brings this claim on behalf of herself and the Class pursuant to the
22 California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200.

23 106. Plaintiff and 23andMe are "persons" within the meaning of Cal. Bus. & Prof. Code
24 §17201.

25 107. The UCL prohibits unfair competition, which includes an "unlawful, unfair or
26 fraudulent" act or practice. Cal. Bus. & Prof. Code §17200.

1 108. Under the UCL, any business act or practice that is unethical, oppressive,
2 unscrupulous, and/or substantially injurious to consumers, or that violates a legislatively declared
3 policy, constitutes an unfair business act or practice.

4 109. The violation of any law constitutes an unlawful business practice under the UCL.

5 110. 23andMe engaged in unfair and unlawful business practices prohibited by the UCL
6 by implementing and maintaining unreasonable data security measures that were inadequate to
7 protect PII and PGI or prevent the Data Breach. These unfair and unlawful practices occurred in
8 connection with 23andMe's trade or business.

9 111. 23andMe's affirmative acts in implementing and maintaining unreasonable data
10 security measures were unfair within the meaning of the UCL, because they constituted immoral,
11 unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers, and
12 provided no benefit to consumers.

13 112. 23andMe's implementation of inadequate and unreasonable data security measures
14 also was unfair within the meaning of the UCL, because its conduct undermined California public
15 policy that businesses protect personal information as reflected in Article I, Section 1 of the
16 California Constitution (enacted because of private sector data processing activity and stating that
17 all people have an inalienable right to privacy) and in statutes such as the Online Privacy Protection
18 Act, Cal. Bus. & Prof. Code §22578 (explaining that the Legislature's intent was to have a uniform
19 policy statewide regarding privacy policies on the Internet); the Information Practices Act, Cal.
20 Civ. Code §1798.1 ("The Legislature declares that. . . all individuals have a right of privacy in
21 information pertaining to them . . . The increasing use of computers. . . has greatly magnified the
22 potential risk to individual privacy that can occur from the maintenance of personal information.");
23 *id.*, §1798.81.5(a)(1); and the FTC Act, 15 U.S.C. §45(a)(1), which prohibits unfair trade practices.

24 113. 23andMe's violations of the California Customer Records Act, Cal. Civ. Code
25 §1798.81.5(b) (the "California Customer Records Act"), moreover, constitute unlawful acts or
26 practices under the UCL. The California Customer Records Act requires a "business that owns,
27 licenses, or maintains personal information about a California resident" to "implement and
28 maintain reasonable security procedures and practices appropriate to the nature of the information"

1 and “to protect the personal information from unauthorized access, destruction, use, modification,
2 or disclosure.” 23andMe failed to implement and maintain such reasonable security procedures
3 and practices before and at the time of the Data Breach. As a result, 23andMe violated the
4 California Customer Records Act, *id.*

5 114. 23andMe’s violations of the FTC Act, 15 U.S.C. §45(a)(1) and California’s Genetic
6 Information Privacy Act, Cal. Civ. Code §56.18 (“GIPA”), also constitute unlawful acts or
7 practices under the UCL. The GIPA requires a “direct-to-consumer genetic testing company” to
8 “[i]mplement and maintain reasonable security procedures and practices to protect a consumer’s
9 genetic data against unauthorized access, destruction, use, modification, or disclosure.”
10 §56.181(d)(1). 23andMe violated §56.181(d)(1) by failing to implement and maintain reasonable
11 security procedures and practices to protect Plaintiff and the Class members’ PGI against
12 unauthorized access, use, and disclosure.

13 115. Plaintiff and the Class reasonably expected 23andMe to implement and maintain
14 reasonable data security measures that complied with industry standards and could prevent the
15 Data Breach and protect PII and PGI.

16 116. Plaintiff and members of the Class had no knowledge and could not have
17 reasonably known that 23andMe implemented and maintained unreasonable data security
18 measures. Because 23andMe was solely responsible for implementing and maintaining reasonable
19 data security measures to protect PII and PGI, neither Plaintiff nor members of the Class could
20 have avoided the injuries they sustained.

21 117. There were reasonably available alternatives to further 23andMe’s legitimate
22 business interests, other than its conduct responsible for the Data Breach.

23 118. 23andMe’s conduct has deprived Plaintiff and members of the Class of their right
24 to control the use and dissemination of their PII and PGI.

25 119. 23andMe willfully engaged in the unfair and unlawful acts and practices described
26 above and knew or should have known that those acts and practices were unfair and unlawful in
27 violation of the UCL.

28

120. As a direct and proximate result of 23andMe's unfair and unlawful practices and violation of UCL, Plaintiff and the Class have suffered injury in fact and have lost money and property. Plaintiff and members of the Class lost money as a result of 23andMe's violation of the GIPA because they paid for a service with reasonable data security measures adequate to protect PII and PGI and prevent the Data Breach but received a service with unreasonable data security measures inadequate to protect PII and PGI or prevent the Data Breach. Plaintiff and members of the Class lost property as a result of 23andMe's violation of the GIPA because they no longer have the exclusive right to control the use and dissemination of their PII and PGI.

121. Plaintiff is entitled to restitution and other relief as this Court considers necessary and proper.

SEVENTH CLAIM FOR RELIEF
Violation of The California Consumer Privacy Act

122. Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

123. Plaintiff brings this claim on behalf of herself and the Class pursuant to the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §1798.100 1798.150.

124. PII and PGI constitute "personal information" within the meaning of *id.*, §1798.81.5(d)(1)(A).

125. The PII and PGI compromised in the Data Breach was nonencrypted and nonredacted.

126. Plaintiff and Class members' PII and PGI was disclosed as a result of 23andMe's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII and PGI of Plaintiff and Class members.

127. 23andMe's misconduct was egregious and serious and has resulted in the violation of the CCPA as to millions of Class members. 23andMe's conduct was intentional insofar as the risk of a data breach and the purported vector of the Data Breach were well-known within the industry and 23andMe intentionally failed to implement or maintain reasonable security measures

adequate to protect Plaintiff and members of the Class's PII and PGI. 23andMe has substantial assets, liabilities, and net worth.

128. On November 2, 2023, Plaintiff sent 23andMe pre-suit notice demand letters, pursuant to *id.*, §1798.150.

129. Plaintiff and members of the Class are entitled to damages and other relief as this Court considers necessary and proper.

EIGHTH CLAIM FOR RELIEF
Unjust Enrichment

130. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

131. Plaintiff brings this claim on behalf of herself and the Class.

132. Plaintiff and members of the Class conferred a benefit on 23andMe in the form of payments made for the purchase of genetic testing kits and in the form of PII and PGI that Plaintiff and Class members provided to 23andMe.

133. 23andMe appreciated or had knowledge of the benefits conferred upon it by Plaintiff and members of the Class. 23andMe continues to store Plaintiff's and Class members' PII and PGI and to derive benefits from such PII and PGI by using it to drive insights that 23andMe can monetize.

134. Under principles of equity and good conscience, 23andMe should not be permitted to retain the benefits of Plaintiff and members of the Class. 23andMe could have but chose not to implement or maintain reasonable data security measures adequate to protect PII and PGI as required by law and industry standards and compromised Plaintiff and Class members' exclusive right to control the use and dissemination of their PII and PGI.

135. Neither Plaintiff nor Class members have an adequate remedy at law. Monetary damages alone are incapable of restoring to Plaintiff or Class members the exclusive right to control the use and dissemination of their PII and PGI, which has been compromised as a direct and proximate result of the Data Breach.

PRAYER FOR RELIEF

136. WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendant and in favor of Plaintiff and the Class and award the following relief:

A. that this action be certified as a class action, pursuant to California Code of Civil Procedure §382, declaring Plaintiff as a representative of the Class and Plaintiff's counsel as counsel for the Class;

B. monetary damages;

C. injunctive relief;

D. reasonable attorneys' fees and expenses, including those related to experts and consultants;

E. costs;

F. pre- and post-judgment interest; and

G. such other relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, demands a trial by jury for all issues so triable.

Dated: December 4, 2023

LEXINGTON LAW GROUP



Mark N. Todzo (Bar No. 168389)
Patrick R. Carey (Bar No. 308623)
Meredyth L. Merrow (Bar No. 328337)
503 Divisadero Street
San Francisco, CA 94117

1 Telephone: (415) 913-7800
2 Facsimile: (415) 759-4112
3 mtodzo@lexlawgroup.com

4 Joseph P. Guglielmo (*pro hac vice* forthcoming)
5 Carey Alexander (*pro hac vice* forthcoming)
6 **SCOTT+SCOTT ATTORNEYS AT LAW LLP**
7 The Helmsley Building
8 230 Park Avenue, 17th Floor
9 New York, NY 10169-1820
10 Telephone: (212) 223-6444
11 Facsimile: (212) 223-6334
12 jguglielmo@scott-scott.com
13 calexander@scott-scott.com

14 *Attorneys for Plaintiff*
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT 2

E-FILED
10/31/2023 9:58 AM
Clerk of Court
Superior Court of CA,
County of Santa Clara
23CV424996
Reviewed By: R. Walker

JASON M. WUCETICH (STATE BAR NO. 222113)
jason@wukolaw.com
DIMITRIOS V. KOROVILAS (STATE BAR NO. 247230)
dimitri@wukolaw.com
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201

Attorneys for Plaintiff
KATHY VASQUEZ, individually and
on behalf of all others similarly situated

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SANTA CLARA

CASE NO. **23CV424996**

KATHY VASQUEZ, individually and on behalf
of all others similarly situated,

Plaintiff,

-v-

23ANDME, INC.,

Defendant.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff Kathy Vasquez (“Plaintiff”), on behalf of herself and all others similarly
2 situated, brings this class Action Complaint (the “Action”) against Defendant 23andMe, Inc.
3 (“23andMe” or “Defendant”), and alleges the following upon information and belief, except as
4 to allegations concerning Plaintiff herself and her actions, which are alleged upon personal
5 knowledge:

6 **I. INTRODUCTION**

7 1. Plaintiff seeks to hold Defendant responsible for the harm it has caused and will
8 continue to cause to Plaintiff and millions of other similarly situated person as a result of
9 Defendant’s inadequate data security policies and practices, which allowed unidentified third
10 parties to download and sell extraordinarily targeted and sensitive personally identifiable
11 information (PII) of Plaintiff and other class members on the Dark Web, including their names,
12 cities and states of residence, genders, years of birth, 23andMe account information, as well as
13 detailed information about Plaintiff and Class Members’ genomics, DNA profile, and
14 information about their ancestry and ethnicity (the “Data Breach”).

15 2. While Defendant has publicly stated that the Data Breach was a result of
16 compromised user credentials whereby attackers gained access to data through passwords that
17 users had reused from other websites that were hacked, that explanation is only a fraction of the
18 story. There should have been no way for any unauthorized third parties to be able to download
19 the sensitive PII of any individuals without being detected and stopped. However, Defendant
20 allowed the sensitive PII *of millions of users* to be downloaded and offered for sale on a Dark
21 Web hacker forum all without Defendant ever detecting this activity. Indeed, Defendant clearly
22 had no security policies or practices in place to detect or stop this Data Breach from occurring.

23 3. Companies entrusted with sensitive personal information, such as Defendant who
24 was entrusted with the detailed genetic information of its customers, should do everything
25 possible to protect against cybersecurity incidents, such as the Data Breach. While Defendant
26 clearly did not maintain adequate cybersecurity policies and practices, Defendant marketed
27 itself as operating a privacy and security-centric business practices. Specifically, Defendant
28

1 represented on its main privacy webpage that “we’re doing everything in our power to keep
2 your personal data safe.”¹

3 4. Moreover, Defendant specifically informed prospective customers that “your
4 personally identifiable information (such as your name and email) is stored in in a separate
5 database from your genetic data so that no one but you (when you use your username and
6 password) can connect the dots between the two”[sic] and that, as a result, “even if someone
7 gained access to one of these databases, they could not connect your identity to your genetic
8 data, or vice versa.”² Defendant also represented to prospective customers that “[w]e meet the
9 highest industry standards for data security. Our information security management system
10 received certification under the globally recognized ISO/IEC 27001:2013, 27018 & 27701
11 standards after an extensive security audit.”³

12 5. Indeed, the Data Breach shows these representations to be false. The hacker(s)
13 here were not only able to access genetic and genomic data for millions of people but, were also
14 able to associate this stolen sensitive PII with the names, years of birth, cities and states of
15 residence, genders, and 23andMe account information of these affected individuals.

16 6. In addition to violating its specific representations to consumers, Defendant’s
17 actions constitute a clear failure to take and implement adequate and reasonable measures to
18 ensure that Plaintiff’s and Class Members’ PII was safeguarded, failing to take available steps
19 to prevent unauthorized disclosure of data, and failing to follow applicable, required, and
20 appropriate protocols, policies, and procedures regarding the encryption of data, even for
21 internal use. Plaintiff and Class Members have a continuing interest in ensuring that their
22 information is and remains safe and are entitled to injunctive and other equitable relief.
23
24
25

26 ¹ See 23andMe “Privacy and Data Protection” webpage, <https://www.23andme.com/privacy/>
27 (last accessed on October 18, 2023).

28 ² *Id.*

³ *Id.*

II. PARTIES

7. Plaintiff Kathy Vasquez is a resident and citizen of California and has been a 23andMe customer since approximately 2021.

8. Defendant 23andMe, Inc. is Delaware corporation with its principal place of business located at 223 N. Mathilda Avenue, Sunnyvale, California 94086.

III. JURISDICTION AND VENUE

9. This Court has general personal jurisdiction over Defendant because, at all relevant times, Defendant is a corporation registered to do business in California with the California Secretary of State. Further, it has had systematic and continuous contacts with the State of California. Defendant is based in Sunnyvale, California, and regularly contracts with a multitude of businesses and organizations in California.

10. Furthermore, this Court has specific personal jurisdiction over Defendant because the claims in this action stem from its specific contacts with the State of California — namely, Defendant’s collection, maintenance, and processing of the personal data of Californians in connection with its business, Defendant’s failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent cybersecurity attack and security breach of such data on or around October 6, 2023 that resulted from Defendant’s failures.

11. Venue is proper in the County of Santa Clara in accordance with Code of Civil Procedure § 395.5 because the alleged wrongs occurred in this county and Defendant conducts business and has its corporate headquarters in Santa Clara County.

IV. STATEMENT OF FACTS

A. Defendant’s Business

12. Defendant is a consumer genetics company founded with the mission “to help people access, understand, and benefit from the human genome.”⁴ Defendant provides

⁴https://investors.23andme.com/?_gl=1*ltxxa*_ga*MTcxMDQzMtYwNC4xNjk3MDQ4MDMx*_ga_G330GF3ZFF*MTY5NzQ5NDM0OS4yLjEuMTY5NzQ5NDM4OC4wLjAuMA.. (last visited Oct. 16, 2023).

consumers with DNA analysis, genetic healthcare information, and genetic ancestry analysis services.

13. In order to use Defendant's services, consumers use a saliva collection kit that Defendant mails to them to collect their saliva at home and mail it back to Defendant's lab in a pre-paid package. Within an average of 3-4 weeks, Defendant analyzes the DNA in the individual's saliva sample and provides detailed personalized reports on everything from the individual's personal genetic health risks and carrier status for various diseases, to the individual's detailed genomics and ancestry profile.⁵

14. The information contained in the individual's genome is then summarized in a report prepared by Defendant which provides an extraordinarily detailed—and intimate—snapshot of the individual's health risks and disease profile. In addition to detailed information about the individual's health and disease profile, the report prepared by Defendant also contains detailed sensitive information about the individual's ethnic and ancestral background.

15. Defendant also provides pharmacogenetics reports that detail how "[individual]' genetics can influence how [the individuals] process certain medications."⁶ Specifically, one type of report Defendant makes available to consumers is called a "Simvastatin Medication Insight report," which provides an analysis of how individuals respond to simvastatin, a commonly-proscribed statin used to lower cholesterol in the blood and reduce the risk of heart attacks, strokes, and heart disease. The report also indicates whether they have an increased chance of experiencing side effects.⁷

B. Defendant's Representations About Security and Privacy

16. Consumers today have dozens of choices for genetic testing services, with some of the leading offerings being AncestryDNA, MyHeritage, Living DNA, FamilyTreeDNA,

⁵ <https://www.23andme.com/genetic-science/> (last visited Oct. 16, 2023).

⁶ See https://www.23andme.com/topics/pharmacogenetics/slco1b1/?_gl=1*1jvwy6o*_ga*MTcxMDQzMTYwNC4xNjk3MDQ4MDMx*_ga_G330GF3ZFF*MTY5NzU2MjU0My4zLjEuMTY5NzU2MzU3MC4wLjAuMA (last visited Oct. 16, 2023).

⁷ *Id.*

1 Nebula Genomics, SelfDecode, and My Toolbox Genomics. In seeking to distinguish itself
2 from the many other genetic testing services available for consumers, Defendant touts its
3 privacy and security practices.

4 17. For example, Defendant tells consumers, in no uncertain terms on the company's
5 primary "About" webpage, that "[y]ou are in control of your DNA and your data," and that
6 "[w]e believe you should have a safe place to explore and understand your genes. That's why
7 Privacy and Security are woven into everything we do."⁸

8 18. On Defendant's Privacy and Data Protection webpage, Defendant elaborates on
9 its practices, saying that "When you explore your DNA with 23andMe, you entrust us with
10 important personal information. That's why, since day one, protecting your privacy has been
11 our number one priority. We're committed to providing you with a safe place where you can
12 learn about your DNA knowing your privacy is protected."⁹ Defendant also states that "[w]e
13 meet the highest industry standards for data security. Our information security management
14 system received certification under the globally recognized ISO/IEC 27001:2013, 27018 &
15 27701 standards after an extensive security audit."¹⁰

16 19. In addition to its claims about privacy protections, Defendant claims to
17 understand and prioritize data security and touts its data security practices as a selling point. For
18 example, Defendant represents that "Your data is fiercely protected by security practices that
19 are regularly reviewed and updated. Your genetic information deserves the highest level of
20 security, because without security, you can't have privacy. 23andMe employs software,
21 hardware, and physical security measures to protect your data." Defendant also represents that
22 "while no security standard or system is bulletproof, we're doing everything in our power to
23 keep your personal data safe."¹¹

24
25 ⁸ See <https://www.23andme.com/about/> (last visited Oct. 16, 2023).

26 ⁹ <https://www.23andme.com/privacy/> (last visited Oct. 16, 2023).

27 ¹⁰ *Id.*

28 ¹¹ *Id.*

20. Defendant has even claimed to understand the need to stay “a step ahead of hackers,” and represented to current and potential customers that it does stay a step ahead of hackers:

“What do you do to stay a step ahead of hackers? We take multiple steps. First of all, third-party security experts regularly conduct audits and assessments of our systems, ensuring we will never let our guard down. We encrypt all sensitive information, both when it is stored and when it is being transmitted, so that we make it difficult for potential hackers to gain access.”¹²

21. To assure any consumers who may still be concerned about sharing their intimate personal and detailed genetic information with Defendant, Defendant represented that personally identifiable information such as name and email could never be connected with genetic data:

“Anything else you can tell me to put my mind at ease?

Rest assured that your personally identifiable information (such as your name and email) is stored in in a separate database from your genetic data so that no one but you (when you use your username and password) can connect the dots between the two. That means even if someone gained access to one of these databases, they could not connect your identity to your genetic data, or vice versa.”¹³

22. Consumers, including Plaintiff and Class Members, relied on Defendant’s representations in choosing Defendant’s services and in agreeing to turn over their DNA, and money, to Defendant.

23. Instead of upholding its promises to current and potential customers, Defendant failed to implement and provide adequate data security policies, measures, and procedures to prevent the unauthorized third-party hackers from downloading the PII, including the sensitive PII of millions of users. Indeed, while Defendant assured consumers that “even if someone gained access to [a genetic database] they could not connect your identity to your genetic data, or vice versa,”¹⁴ the Data Breach has showed that representation to false and that Plaintiff’s and

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

Class Members’ genetic information was easily stolen, sold, and associated with their names and identifying information by the hackers.

C. The Data Breach

24. In an announcement posted to 23andMe’s website on October 6, 2023 (the “Announcement”), 23andMe explains:

“We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users’ authorization.

After learning of suspicious activity, we immediately began an investigation. While we are continuing to investigate this matter, we believe threat actors were able to access certain accounts in instances where users recycled login credentials – that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked,

We believe the treat actor may have then, in violation of our Terms of Service, accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users’ DNA Relatives profiles, to the extent a user opted into that service.”¹⁵

25. Defendant’s Announcement failed to provide additional information, including the number of affected individuals or the specific types of information available. However, numerous sources, including some from the Dark Web, show that at least 999,998 individuals were affected by the Data Breach, including Plaintiff and Class Members, that likely more than 7 million users are implicated, and that the hacker clearly targeted individuals of Ashkenazi Jewish decent.

26. On or around October 3, 2023, the hacker responsible for the cyberattack posted on a Dark Web hacker forum claiming to have data for 7 million users—i.e., half of the members of 23andMe—including information about origin estimation, phenotype and health information. To validate the hacker’s claim to have this extremely sensitive genetic data, the hacker posted a spreadsheet entitled “Ashkenazi DNA Data of Celebrities” that contained the

¹⁵ See <https://blog.23andme.com/articles/addressing-data-security-concerns> (last visited October 18, 2023).

names and sensitive PII, including genetic information, for 999,998 individuals, including Plaintiff.

27. The PII in the sample spreadsheet posted online includes the name, gender, birth year, profile_id, account_id, location, and ancestral background information of approximately one million individuals of Ashkenazi Jewish decent. It also includes the Y-chromosome haplogroup for all male individuals listed and the mitochondrial DNA haplogroup for all of the listed individuals. These haplogroups provide a specific identification of the ancestral/genetic group that the individuals fall into and can be used to understand not only the specific ancestral lineage(s) the individual belongs in but also likely health-and disease-affecting genetic mutations the individual is likely to possess.

28. In addition to the spreadsheet labeled as containing “Ashkenazi DNA,” reports indicate that the 23andMe-derived genetic data of more than 300,000 individuals of Chinese heritage has already been disclosed.¹⁶

D. Defendant Violated Its Obligations to Plaintiff and Class Members

29. The Data Breach exposed Defendant’s inadequate cybersecurity and privacy practices as woefully insufficient. While Defendant’s announcement states that the information is information the individuals “opted into sharing through [Defendant’s] DNA Relatives feature,” Plaintiff and Class Members never opted into having this sensitive PII shared with the any unauthorized individuals, and certainly not cybercriminals.

30. More fundamentally, no company entrusted with such intimate personal information, such as Defendant, should have allowed a bad actor to abuse a feature meant to allow people to find and connect with their relatives in order to download the PII of millions of users. Any adequate cybersecurity protocol would have detected the hacker’s viewing and exfiltration of a few dozen people’s PII and alerted the company and/or cut off access. However, Defendant had no such protections and allowed the actor to exfiltrate the information of more than half of Defendant’s customers without being caught.

¹⁶ See <https://therecord.media/scraping-incident-genetic-testing-site> (last visited Oct. 18, 2023).

1 31. Indeed, the fact that Defendant only announced the Data Breach four days after
2 the hacker posted the stolen PII on a hacking forum suggests that Defendant only “learned” of
3 the Data Breach after the hacker posted, and sold, the information to the Dark Web and not
4 through any security alerts or detectors on Defendant’s systems.

5 32. As a direct result of Defendant’s failure to secure and safeguard the sensitive
6 information of customers that entrusted them to do so, all of this sensitive PII is in the hands of
7 cybercriminals. In fact, for the 999,998 Ashkenazi Jewish individuals and roughly 300,000
8 Chinese individuals, including Plaintiff, whose sensitive PII was already posted, the PII is now
9 in the hands of cybercriminals and is readily available to download by anyone with access to the
10 hacking forum.

11 33. At all relevant times, Defendant had a duty to Plaintiff and Class Members by
12 properly securing their PII, encrypt and maintain such information using industry standard
13 methods, train its employees, utilize available technology to defend its systems from invasion,
14 act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly
15 notify Plaintiff and Class Members when Defendant became aware that their PII may have been
16 compromised.

17 34. Defendant’s duty to use reasonable security measures arose as a result of the
18 special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class
19 Members, on the other hand. The special relationship arose because Plaintiff and the Members
20 of the Class relied on Defendant to secure their PII when they entrusted Defendant with the
21 information required to obtain Defendant’s services.

22 35. Defendant had the resources necessary to prevent the Data Breach but neglected
23 to adequately invest in adequate security measures, despite its obligation to protect customers’
24 PII. Accordingly, Defendant breached its common law, statutory, and other duties owed to
25 Plaintiff and Class Members.
26
27
28

36. Defendant owed a non-delegable duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information against unauthorized access and disclosure.

37. In fact, as detailed above, Defendant's failure to implement and maintain adequate security measures also violated Defendant's representations and promises to its current and prospective customers, on which Plaintiff and Class Members relied in choosing to (i) provide their genetic information to Defendant, (ii) allow Defendant to analyze their DNA to generate summaries of their health and ancestry-related genetics, and (iii) pay Defendant for such services.

38. As a result of the Data Breach, Plaintiff and Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, lost money paid to Defendant, and the loss of, and diminution in, value of their PII.

39. In addition, Plaintiff's and Class Members' sensitive PII, while compromised and taken by unauthorized third parties, also remains in Defendant's possession. Without additional safeguards and independent review and oversight, it remains vulnerable to future cyberattacks and theft.

40. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect victims' PII.

41. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant and entities like it, and Defendant was thus on notice that failing to take steps necessary to secure the PII against those risks left that property in a dangerous condition and vulnerable to theft. Defendant was further on notice of the severe consequences that would result to Plaintiff and Class Members from its failure to safeguard their PII.

42. Defendant failed to properly monitor the computer network and systems that stored the PII. Instead, had Defendant properly monitored its computer network and systems, it would have discovered the intrusion sooner and could have cut off access to the hacker(s) thereby mitigating the impact of the attack, as opposed to letting cyberthieves roam freely in Defendant's network for an unknown period of time.

43. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

44. Plaintiff and Class Members will incur out of pocket costs for undertaking protective measures to deter and detect identity theft.

45. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

46. Plaintiff seeks remedies including, but not limited to, actual damages, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of herself and the Class.

E. Defendant Failed to Comply with FTC Guidelines

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

48. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on

1 computer networks; understand their network’s vulnerabilities; and implement policies to
2 correct any security problems.¹⁷

3 49. The guidelines also recommend that businesses use an intrusion detection system
4 to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating
5 someone is attempting to hack the system; watch for large amounts of data being transmitted
6 from the system; and have a response plan ready in the event of a breach.¹⁸

7 50. The FTC further recommends that companies limit access to sensitive data;
8 require complex passwords to be used on networks; use industry-tested methods for security;
9 monitor for suspicious activity on the network; and verify that third-party service providers
10 have implemented reasonable security measures.

11 51. The FTC has brought enforcement actions against businesses for failing to
12 adequately and reasonably protect customer data, treating the failure to employ reasonable and
13 appropriate measures to protect against unauthorized access to confidential consumer data as an
14 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),
15 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must
16 take to meet their data security obligations.

17 52. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits “unfair . . . practices in or
18 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or
19 practice by businesses, such as Defendant, of failing to use reasonable measures to protect
20 personal, private Information. The FTC publications and orders described above also form part
21 of the basis of Defendant’s duty in this regard.

22 53. Defendant’s failure to employ reasonable and appropriate measures to protect
23 against unauthorized access to Plaintiff’s and Class Members’ PII or to comply with applicable
24

25
26 ¹⁷ See *Protecting Personal Information: A Guide for Business*, Federal Trade Commission
27 (2016), available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
28 0136_proteting-personal-information.pdf (last visited Oct. 17, 2023).

¹⁸ *Id.*

1 industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15
2 U.S.C. § 45.

3 54. Defendant was at all times fully aware of its obligation to protect the Private
4 Information of its customers, Defendant was also aware of the significant repercussions that
5 would result from its failure to do so. Accordingly, Defendant's conduct was particularly
6 unreasonable given the nature and amount of PII it obtained and stored and the foreseeable
7 consequences of the immense damages that would result to Plaintiff and the Class.

8 **F. Plaintiff Kathy Vasquez**

9 55. Plaintiff Kathy Vasquez is, and at all times relevant, has been a resident and
10 citizen of California. Plaintiff received two emails from Defendant on or around October 12,
11 2023, notifying her that her information was exposed in the Data Breach.

12 56. Plaintiff provided her PII to Defendant directly in order to obtain ancestry tracing
13 and genomic services from Defendant.

14 57. Plaintiff paid Defendant money in exchange for these services.

15 58. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff
16 has never knowingly transmitted unencrypted sensitive PII over the internet or any other
17 unsecured source.

18 59. As detailed above, Plaintiff received two emails directly from Defendant
19 confirming that her PII had been improperly accessed and/or obtained by unauthorized third
20 parties while in possession of Defendant.

21 60. The Data Breach email indicated that, while the investigation is ongoing,
22 Defendant believes that a threat actor was able to access certain accounts in instances where
23 users employed identical login credentials but does not mention the specific types of PII being
24 affected.

25 61. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the
26 impact of the Data Breach after receiving the data breach notification email including but not
27 limited to researching the Data Breach; reviewing credit reports, financial account statements,
28

1 and/or medical records for any indications of actual or attempted identity theft or fraud;
2 switching her VPN provider; and researching and purchasing additional antivirus, Dark Web
3 monitoring, and/or credit monitoring services.

4 62. Since the Data Breach, Plaintiff has received increased email spam, increased
5 scammer telephone calls and increased scammer text messages. Her father and aunt were also
6 contacted and told Plaintiff had been kidnapped and demanded ransom.

7 63. Plaintiff has spent hours addressing the Data Breach and will continue to spend
8 valuable time for the remainder of her life, that she otherwise would have spent on other
9 activities, including but not limited to work and/or recreation.

10 64. Plaintiff suffered actual injury from having her PII compromised as a result of
11 the Data Breach including, but not limited to (a) damage to and diminution in the value of her
12 PII, a form of property that Defendant maintained belonging to Plaintiff; (b) violation of her
13 privacy rights; (c) the theft of her PII; (d) lost money paid to Defendant and the lost benefit of
14 the bargain in Defendant's failure to comply with its obligations and representations, (e) the
15 out-of-pocket costs of purchasing additional identity theft protection, antivirus, Dark Web
16 monitoring, and/or credit monitoring software; and (f) present, imminent and impending injury
17 arising from the increased risk of identity theft and fraud. In fact, because her genetic data was
18 impacted, and because her PII was sold and exchanged on the Dark Web, Plaintiff faces this risk
19 for her lifetime.

20 65. As a result of the Data Breach, Plaintiff has also suffered emotional distress as a
21 result of the release of her PII, which she believed would be protected from unauthorized access
22 and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her
23 PII for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and
24 fraud, as well as the consequences of such identity theft and fraud resulting from the Data
25 Breach which was maliciously targeted at individuals that share Plaintiff's genetic heritage.

26 66. As a result of the Data Breach, Plaintiff anticipates spending considerable time
27 and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach.
28

1 In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of
2 identity theft and fraud for the remainder of her life.

3 **V. CLASS ALLEGATIONS**

4 67. Plaintiff brings this action on behalf of herself and all other similarly situated
5 persons pursuant to California Code of Civil Procedure § 382. Plaintiff seek to represent the
6 following class:

7 All citizens of the State of California whose personal information was compromised in or
8 as a result of the data breach of Defendant announced on or around October 6, 2023.

9 68. Excluded from the Classes are the following individuals and/or entities:
10 Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors and any entity
11 in which Defendant has a controlling interest, all individuals who make a timely election to be
12 excluded from this proceeding using the correct protocol for opting out, any and all federal,
13 state or local governments, including but not limited to its departments, agencies, divisions,
14 bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear
15 any aspect of this litigation, as well as their immediate family members.

16 69. In the alternative, Plaintiff requests additional subclasses as necessary based on
17 the types of PII that were compromised.

18 70. This action has been brought and may be maintained as a class action under
19 California Code of Civil Procedure § 382 because there is a well-defined community of interest
20 in the litigation and the proposed classes are ascertainable, as described further below:

- 21 a. Numerosity: A class action is the only available method for the fair and efficient
22 adjudication of this controversy. The members of the Class are so numerous that
23 joinder of all members is impractical, if not impossible. Plaintiff is informed and
24 believes and, on that basis, alleges that the total number of Class Members is at
25 least in the hundreds of thousands of individuals. Membership in the Class will
26 be determined by analysis of Defendant's records and/or through the records
27 made publicly available by the bad actor(s).

1 b. Commonality: Plaintiff and the Class Members share a community of interest in
2 that there are numerous common questions and issues of fact and law which
3 predominate over any questions and issues solely affecting individual members,
4 including, but not necessarily limited to:

- 5 i. Whether Defendant had a legal duty to Plaintiff and the Class to exercise
6 due care in collecting, storing, using and/or safeguarding their PII;
- 7 ii. Whether Defendant knew or should have known of the susceptibility of
8 its data security systems to a data breach;
- 9 iii. Whether Defendant's security procedures and practices to protect its
10 systems were reasonable in light of the measures recommended by data
11 security experts;
- 12 iv. Whether Defendant's failure to implement adequate data security
13 measures allowed the Data Breach to occur;
- 14 v. Whether Defendant failed to comply with its own policies and applicable
15 laws, regulations and industry standards relating to data security);
- 16 vi. Whether Defendant adequately, promptly and accurately informed
17 Plaintiff and Class Members that their PII had been compromised;
- 18 vii. How and when Defendant actually learned of the Data Breach;
- 19 viii. Whether Defendant's conduct, including its failure to act, resulted in or
20 was the proximate cause of the breach of its systems, resulting in the loss
21 of the PII of Plaintiff and Class Members;
- 22 ix. Whether Defendant adequately addressed and fixed the vulnerabilities
23 which permitted the Data Breach to occur;
- 24 x. Whether Defendant engaged in unfair, unlawful or deceptive practices by
25 failing to safeguard Plaintiff's and Class Members' PII;
- 26 xi. Whether Plaintiff and Class Members are entitled to actual and/or
27 statutory damages and/or whether injunctive, corrective and/or
28

1 declaratory relief and/or an accounting is/are appropriate as a result of
2 Defendant's wrongful conduct;

3 xii. Whether Plaintiff and Class Members are entitled to restitution as a result
4 of Defendant's wrongful conduct.

5 c. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and
6 all members of the Class sustained damages arising out of and caused by
7 Defendant's common course of conduct in violation of law, as alleged herein.

8 d. Adequacy of Representation: Plaintiff in this class action is an adequate
9 representative of the Class in that Plaintiff has the same interest in the litigation
10 of this case as the Class Members, are committed to the vigorous prosecution of
11 this case and have retained competent counsel who are experienced in
12 conducting litigation of this nature. Plaintiff is not subject to any individual
13 defenses unique from those conceivably applicable to other Class Members or
14 the Class in their entirety. Plaintiff anticipates no management difficulties in this
15 litigation.

16 e. Superiority of Class Action: The damages suffered by individual Class Members
17 are significant but may be small relative to each member's enormous expense of
18 individual litigation. This makes or may make it impractical for members of the
19 Class to seek redress individually for the wrongful conduct alleged herein. Even
20 if Class Members could afford such individual litigation, the court system could
21 not. Should separate actions be brought or be required to be brought by each
22 individual member of the Class, the resulting multiplicity of lawsuits would
23 cause undue hardship and expense for the Court and the litigants. The
24 prosecution of separate actions would also create a risk of inconsistent rulings
25 which might be dispositive of the interests of other Class Members who are not
26 parties to the adjudications and/or may substantially impede their ability to
27 protect their interests adequately. Individualized litigation increases the delay
28

and expense to all parties and to the court system, presented by the case's complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

71. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, so it is impracticable to bring all Class Members before the Court.

72. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Classes in their entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly. Plaintiff's challenge of these policies and practices hinges on Defendant's conduct concerning the Classes in their entirety, not on facts or law applicable only to Plaintiff.

CAUSES OF ACTION

COUNT ONE **(Negligence)**

73. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

74. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Plaintiff's and Class Members' PII on its computer systems and networks.

75. The duty Defendant owed Plaintiff and Class Members includes but is not limited to (a) the duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession; (b) the duty to protect Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices and/or its own representations; (c) the duty to

1 implement processes to detect the Data Breach quickly and to act on warnings about data
2 breaches timely; and (d) the duty to promptly notify Plaintiff and Class Members of any data
3 breach, security incident or intrusion that affected or may have affected their PII.

4 76. Defendant knew or should have known that the PII was private and confidential
5 and should be protected as private and confidential and, thus, Defendant owed a duty of care to
6 not subject Plaintiff and Class Members to an unreasonable risk of harm because they were
7 foreseeable and probable victims of any inadequate security practices.

8 77. Defendant knew or should have known of the risks inherent in collecting and
9 storing PII, the vulnerabilities of its data security systems and the importance of adequate
10 security. Defendant knew or should have known about numerous well-publicized data breaches,
11 including breaches dealing with genetic information of individuals.

12 78. Defendant knew or should have known that its data systems and networks did
13 not adequately safeguard Plaintiff's and Class Members' PII.

14 79. Because Defendant knew that a breach of its systems could damage numerous
15 individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect
16 its data systems and the PII stored thereon.

17 80. Only Defendant was in the position to ensure that its systems and protocols were
18 sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

19 81. Defendant breached its duties to Plaintiff and Class Members by failing to
20 provide fair, reasonable, or adequate computer systems and data security practices to safeguard
21 their PII. This breach of duty includes but is not limited to (a) failing to implement computer
22 systems and data security practices to detect the intrusion and downloading of PII for millions
23 of Defendant's customers; (b) failing to timely and accurately disclose that Plaintiff's and Class
24 Members' PII had been improperly acquired or accessed; (c) failing to provide adequate
25 supervision and oversight of the PII with which it was and is entrusted, in spite of the known
26 risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party
27 to gather Plaintiff's and Class Members' PII, misuse the PII and intentionally disclose it to
28

1 others without consent; (d) failing to adequately train its employees with respect to security
2 practices that would have prevented or mitigated the extent of the Data Breach; (e) failing to
3 adequately enforce security policies aimed at protecting Plaintiff's and Class Members' PII; and
4 (f) failing to implement processes to quickly detect data breaches, security incidents or
5 intrusions such as the Data Breach in question.

6 82. As a proximate and foreseeable result of Defendant's negligent conduct, Plaintiff
7 and Class Members have suffered damages and are at imminent risk of additional harm and
8 damages (as alleged above).

9 83. Further, by explicitly failing to provide timely and clear notification of the Data
10 Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from
11 taking meaningful, and proactive steps to secure their PII.

12 84. There is a close causal connection between Defendant's failure to implement
13 security measures to protect Plaintiff's and Class Members' PII and the harm (or risk of
14 imminent harm suffered) by Plaintiff and Class Members. Plaintiff's and Class Members' PII
15 was accessed as the proximate result of Defendant's failure to exercise reasonable care in
16 safeguarding such PII by adopting, implementing, and maintaining appropriate security
17 measures.

18 85. Defendant's wrongful actions, inactions, and omissions constituted (and continue
19 to constitute) common law negligence.

20 86. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
21 Members have suffered and will continue to suffer injury, including but not limited to (a)
22 damage to and diminution in the value of their PII, a form of property that Defendant
23 maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c)
24 (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and
25 the lost benefit of the bargain in Defendant's failure to comply with its obligations and
26 representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of
27
28

1 the Data Breach; and (f) the present, imminent and impending injury arising from the increased
2 risk of identity theft and fraud.

3 87. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
4 Members have suffered and will continue to suffer other forms of injury and/or harm, including
5 but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-
6 economic losses.

7 88. Additionally, as a direct and proximate result of Defendant's negligence,
8 Plaintiff and Class Members have suffered and will continue to suffer the continued risks of
9 exposure of their PII, which remains in Defendant's possession and is subject to further
10 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
11 measures to protect PII in its continued possession.

12 **COUNT TWO**
13 **(Breach of Implied Contract)**

14 89. Each and every allegation of the preceding paragraphs is incorporated in this
15 Count with the same force and effect as though fully set forth herein.

16 90. Through their course of conduct, Defendant, Plaintiff, and Class Members
17 entered into implied contracts for Defendant to implement data security adequate to safeguard
18 and protect the privacy of Plaintiff's and Class Members' PII.

19 91. Defendant required Plaintiff and Class Members to provide and entrust their PII
20 to it as a condition of obtaining Defendant's services.

21 92. Defendant solicited and invited Plaintiff and Class Members to provide their PII
22 as part of Defendant's regular business practices. Plaintiff and Class Members accepted
23 Defendant's offers and provided their PII to Defendant.

24 93. As a part of the agreement, as discussed above, Defendant specifically agreed
25 that it would provide security to detect and prevent data breaches and misuse of Plaintiff's and
26 Class Members' PII, to safeguard and protect such non-public information, and to keep such
27 information secure and confidential. Defendant also impliedly agreed to timely and accurately
28 notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

1 failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members, and
2 continued acceptance of PII and storage of other personal information after Defendant knew or
3 should have known of the security vulnerabilities of the systems that were exploited in the Data
4 Breach.

5 102. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff
6 and Class Members the full benefit of their bargains as originally intended by the parties,
7 thereby causing them injury in an amount to be determined at trial.

8 **COUNT FOUR**
9 **(Unjust Enrichment)**

10 103. Each and every allegation of the preceding paragraphs is incorporated in this
11 Count with the same force and effect as though fully set forth herein.

12 104. Plaintiff and Class Members conferred a monetary benefit on Defendant.
13 Specifically, they purchased goods and services from Defendant and in so doing provided
14 Defendant with their Private Information. In exchange, Plaintiff and Class Members should
15 have received from Defendant the goods and services that were the subject of the transaction
16 and have their PII protected with adequate data security.

17 105. Defendant knew that Plaintiff and Class Members conferred a benefit which
18 Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and
19 Class Members for business purposes.

20 106. The amounts Plaintiff and Class Members paid for goods and services were used,
21 in part, to pay for use of Defendant's network and the administrative costs of data management
22 and security.

23 107. Under the principles of equity and good conscience, Defendant should not be
24 permitted to retain the money belonging to Plaintiff and Class Members, because Defendant
25 failed to implement appropriate data management and security measures that are mandated by
26 industry standards and by Defendant's own representations to Plaintiff and Class Members.
27
28

1 108. Defendant failed to secure Plaintiff's and Class Members' Private Information
2 and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members
3 provided.

4 109. Defendant acquired the PII through inequitable means in that it failed to disclose
5 the inadequate security practices previously alleged.

6 110. If Plaintiff and Class Members knew that Defendant had not reasonably secured
7 their PII, they would not have agreed to Defendant's services.

8 111. Plaintiff and Class Members have no adequate remedy at law.

9 112. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
10 Members have suffered and will continue to suffer injury, including but not limited to (a)
11 damage to and diminution in the value of their PII, a form of property that Defendant
12 maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c)
13 (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and
14 the lost benefit of the bargain in Defendant's failure to comply with its obligations and
15 representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of
16 the Data Breach; and (f) the present, imminent, and impending injury arising from the increased
17 risk of identity theft and fraud.

18 113. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
19 Members have suffered and will continue to suffer injury, including but not limited to (a)
20 damage to and diminution in the value of their PII, a form of property that Defendant
21 maintained belonging to Plaintiff and Class Members; (b) violation of their privacy rights; (c)
22 (iii) the compromise, publication, and/or theft of their PII; (d) lost money paid to Defendant and
23 the lost benefit of the bargain in Defendant's failure to comply with its obligations and
24 representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of
25 the Data Breach; and (f) the present, imminent, and impending injury arising from the increased
26 risk of identity theft and fraud.

114. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

115. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT FIVE
**(Violation of the California Unfair Competition Law,
 Cal. Bus. & Prof. Code § 17200, *et seq.*)**

116. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

117. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200 *et seq.* ("UCL"), prohibits any "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

118. By reason of Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, as described above, and the unauthorized disclosure of Plaintiff and Class Members' PII, Defendant engaged in unfair practices within the meaning of the UCL.

119. Defendant has violated the UCL by engaging in unfair business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in the UCL with respect to the services provided to the Class.

120. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the PII of Plaintiff and Class Members has been compromised.

121. Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Class Members' PII also constitute "unfair" business acts and practices within the meaning the UCL in that Defendant's conduct was substantially injurious to Plaintiff and Class Members, offensive to public policy,

1 immoral, unethical, oppressive and unscrupulous, and the gravity of Defendant's conduct
2 outweighs any alleged benefits attributable to such conduct.

3 122. Defendant's business practices as alleged herein are wrongful and unfair
4 because, through the specific statements described above, Defendant is likely to mislead
5 consumers into believing that the PII they provided to Defendant will remain private and secure,
6 when in fact it has not been maintained in a private and secure manner, that Defendant would
7 employ computer systems and practices to prevent the access to and downloading of millions of
8 users' PII, when in fact it did not, and that Defendant would take proper measures to investigate
9 and remediate a data breach such as, when Defendant did not do so.

10 123. Plaintiff and Class Members suffered (and continue to suffer) injury in fact and
11 lost money or property as a direct and proximate result of Defendant's unfair competition and
12 violation of the UCL, including but not limited to the price received by Defendant for the
13 services, the loss of Plaintiff's and Class Members' legally protected interest in the
14 confidentiality and privacy of their Private Information, nominal damages, and additional losses
15 as described above.

16 124. Plaintiff, on behalf of the Class, seeks relief under the UCL, including, but not
17 limited to, restitution to Plaintiff and Class Members of money or property that Defendant may
18 have acquired by means of Defendant's unfair and fraudulent business practices, restitutionary
19 disgorgement of all profits accruing to Defendant because of Defendant's unfair business
20 practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc.
21 §1021.5), and injunctive or other equitable relief.

22 **COUNT SIX**
23 **(Violation of the California Consumer Privacy Act,**
24 **Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a)**
25 **By Plaintiff and the Class Against All Defendants)**

26 125. Plaintiff realleges and incorporates by reference the preceding paragraphs as
27 though fully set forth herein.
28

1 126. The California Consumer Privacy Act (“CCPA”), Cal. Civ. Code § 1798.150(a),
2 creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically
3 provides:

4 Any consumer whose nonencrypted and nonredacted personal information, as
5 defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section
6 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or
7 disclosure as a result of the business’s violation of the duty to implement and
8 maintain reasonable security procedures and practices appropriate to the nature of
the information to protect the personal information may institute a civil action for
any of the following:

9 (A) To recover damages in an amount not less than one hundred dollars
10 (\$100) and not greater than seven hundred and fifty (\$750) per consumer
per incident or actual damages, whichever is greater.

11 (B) Injunctive or declaratory relief.

12 (C) Any other relief the court deems proper.

13
14 127. Defendant is a “business” under § 1798.140(b) in that it is a corporation organized
15 for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of
16 \$25 million.

17 128. Plaintiff and class members are covered “consumers” under § 1798.140(g) in that
18 they are natural persons who are California residents.

19 129. The personal information of Plaintiff and class members at issue in this lawsuit
20 constitutes “personal information” under § 1798.150(a) and 1798.81.5, in that the personal
21 information Defendant collects and which was impacted by the cybersecurity attack includes an
22 individual’s first name or first initial and the individual’s last name in combination with one or
23 more of the following data elements, with either the name or the data elements not encrypted or
24 redacted: (i) Social security number; (ii) Driver’s license number, California identification card
25 number, tax identification number, passport number, military identification number, or other
26 unique identification number issued on a government document commonly used to verify the
27 identity of a specific individual; (iii) account number or credit or debit card number, in
28

1 combination with any required security code, access code, or password that would permit access
2 to an individual's financial account; (iv) medical information; (v) health insurance information;
3 (vi) unique biometric data generated from measurements or technical analysis of human body
4 characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific
5 individual; (vii) genetic data.

6 130. Defendant knew or should have known that its computer systems and data
7 security practices were inadequate to safeguard the Plaintiff's and class members' personal
8 information and that the risk of a data breach or theft was highly likely. Defendant failed to
9 implement and maintain reasonable security procedures and practices appropriate to the nature of
10 the information to protect the personal information of Plaintiff and the class. Specifically,
11 Defendant subjected Plaintiff's and class members' nonencrypted and nonredacted personal
12 information to an unauthorized access and exfiltration, theft, or disclosure as a result of the
13 Defendant's violation of the duty to implement and maintain reasonable security procedures and
14 practices appropriate to the nature of the information, as described herein.

15 131. As a direct and proximate result of Defendant's violation of its duty, the
16 unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and class members'
17 personal information included exfiltration, theft, or disclosure through Defendant's servers,
18 systems, and website, and/or the dark web, where hackers further disclosed Defendant's
19 customers' and their employees' personal information.

20 132. As a direct and proximate result of Defendant's acts, Plaintiff and class members
21 were injured and lost money or property, the loss of Plaintiff's and the class's legally protected
22 interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety,
23 nominal damages, and additional losses described above.

24 133. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be
25 required prior to an individual consumer initiating an action solely for actual pecuniary
26 damages." Accordingly, Plaintiff and the class by way of this complaint seek actual pecuniary
27 damages suffered as a result of Defendant's violations described herein. Plaintiff has issued
28

1 and/or will issue a notice of these alleged violations pursuant to § 1798.150(b) and intends to
 2 amend this complaint to seek statutory damages and injunctive relief upon expiration of the 30-
 3 day cure period pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b).

4 **COUNT SEVEN**

5 **(Violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, 6 By Plaintiff and the Class Against All Defendants)**

7 134. Plaintiff realleges and incorporates by reference the preceding paragraphs as
 8 though fully set forth herein.

9 135. Cal. Civ. Code § 1798.81.5 provides that “[i]t is the intent of the Legislature to
 10 ensure that personal information about California residents is protected. To that end, the purpose
 11 of this section is to encourage businesses that own, license, or maintain personal information
 12 about Californians to provide reasonable security for that information.”

13 136. Section 1798.81.5(b) further states that: “[a] business that owns, licenses, or
 14 maintains personal information about a California resident shall implement and maintain
 15 reasonable security procedures and practices appropriate to the nature of the information, to
 16 protect the personal information from unauthorized access, destruction, use, modification, or
 17 disclosure.”

18 137. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of
 19 this title may institute a civil action to recover damages.” Section 1798.84(e) further provides
 20 that “[a]ny business that violates, proposes to violate, or has violated this title may be enjoined.”

21 138. Plaintiff and members of the class are “customers” within the meaning of Civ.
 22 Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal
 23 information to Defendant.

24 139. The personal information of Plaintiff and the class at issue in this lawsuit
 25 constitutes “personal information” under § 1798.81.5(d)(1) in that the personal information
 26 Defendant collects and which was impacted by the cybersecurity attack includes an individual’s
 27 first name or first initial and the individual’s last name in combination with one or more of the
 28

1 following data elements, with either the name or the data elements not encrypted or redacted: (i)
2 Social security number; (ii) Driver's license number, California identification card number, tax
3 identification number, passport number, military identification number, or other unique
4 identification number issued on a government document commonly used to verify the identity of
5 a specific individual; (iii) account number or credit or debit card number, in combination with
6 any required security code, access code, or password that would permit access to an individual's
7 financial account; (iv) medical information; (v) health insurance information; (vi) unique
8 biometric data generated from measurements or technical analysis of human body characteristics,
9 such as a fingerprint, retina, or iris image, used to authenticate a specific individual; (vii) genetic
10 data.

11 140. Defendant knew or should have known that its computer systems and data
12 security practices were inadequate to safeguard the class's personal information and that the risk
13 of a data breach or theft was highly likely. Defendant failed to implement and maintain
14 reasonable security procedures and practices appropriate to the nature of the information to
15 protect the personal information of Plaintiff and the class. Specifically, Defendant failed to
16 implement and maintain reasonable security procedures and practices appropriate to the nature of
17 the information, to protect the personal information of Plaintiff and the class from unauthorized
18 access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and
19 the class's nonencrypted and nonredacted personal information to an unauthorized access and
20 exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement
21 and maintain reasonable security procedures and practices appropriate to the nature of the
22 information, as described herein.

23 141. As a direct and proximate result of Defendant's violation of its duty, the
24 unauthorized access, destruction, use, modification, or disclosure of the personal information of
25 Plaintiff and the class included hackers' access to, removal, deletion, destruction, use,
26 modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and
27
28

the class by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

142. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the class were injured and lost money or property, including but not limited to the loss of Plaintiff's and the class's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

143. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

144. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

- a. The name and contact information of the reporting person or business subject to this section;
- b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- c. If the information is possible to determine at the time the notice is provided, then any of the following:
 - i. the date of the breach,
 - ii. the estimated date of the breach, or
 - iii. the date range within which the breach occurred. The notification shall also include the date of the notice;
- d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

- e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;
- f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;
- g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

145. Plaintiff and class members were entitled to receive timely notice from Defendant.

146. On information and belief, many class members affected by the breach, have not received any notice at all from Defendant in violation of Section 1798.82(d).

147. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and class members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

148. As a direct consequence of the actions as identified above, Plaintiff and class members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred but for the data breach of Defendant, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. An order certifying the class pursuant to California Code of Civil Procedure § 382 and declaring that Plaintiff is the class representative and appointing Plaintiff's counsel as class counsel;
2. Permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. Compensatory, consequential, general, and nominal damages in an amount to be proven at trial;
4. Disgorgement and restitution of all earnings, profits, compensation, and benefits received as a result of the unlawful acts, omissions, and practices described herein;
5. Punitive, exemplary, and/or trebled damages to the extent permitted by law;
6. Plaintiff intends to amend this complaint to seek statutory damages upon expiration of the 30-day cure period pursuant to Cal. Civ. Code § 1798.150(b);
7. A declaration of right and liabilities of the parties;
8. Costs of suit;
9. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code § 1021.5;
10. Pre- and post-judgment interest at the maximum legal rate;
11. Distribution of any monies recovered on behalf of members of the class or the general public via fluid recovery or *cy pres* recovery where necessary and as applicable to prevent Defendant from retaining the benefits of their wrongful conduct; and

///

12. Such other relief as the Court deems just and proper.

Dated: October 31, 2023

WUCETICH & KOROVILAS LLP



By: _____

Jason M. Wucetich
Attorneys for Plaintiff Kathy Vasquez,
individually and on behalf of
all others similarly situated

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the class, hereby demands a trial by jury on all issues of fact or law so triable.

Dated: October 31, 2023

WUCETICH & KOROVILAS LLP

By: 

Jason M. Wucetich
Attorneys for Plaintiff Kathy Vasquez,
individually and on behalf of
all others similarly situated

EXHIBIT 3

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SANTA CLARA

**191 N. FIRST STREET
SAN JOSE, CA 95113-1090**

**Electronically Filed
by Superior Court of CA,
County of Santa Clara,
on 11/29/2023 1:33 PM
Reviewed By: R. Walker
Case #23CV424996
Envelope: 13716827**

TO: FILE COPY

RE: **Vasquez v. 23andMe, Inc. (Class Action)**

CASE NUMBER: **23CV424996**

**ORDER DEEMING CASE COMPLEX AND STAYING DISCOVERY
AND RESPONSIVE PLEADING DEADLINE**

WHEREAS, the Complaint was filed by Plaintiff **Kathy Vasquez** ("Plaintiff") in the Superior Court of California, County of Santa Clara, on **October 31, 2023** and assigned to Department **1** (Complex Civil Litigation), the **Honorable Sunil R. Kulkarni** presiding, pending a ruling on the complexity issue;

IT IS HEREBY ORDERED that:

The Court determines that the above-referenced case is **COMPLEX** within the meaning of California Rules of Court 3.400. The matter remains assigned, for all purposes, including discovery and trial, to Department **1** (Complex Civil Litigation), the **Honorable Sunil R. Kulkarni** presiding.

The parties are directed to the Court's local rules and guidelines regarding electronic filing and to the Complex Civil Guidelines, which are available on the Court's website.

Pursuant to California Rules of Court, Rule 3.254, the creation and maintenance of the Master Service List shall be under the auspices of (1) Plaintiff **Kathy Vasquez**, as the first-named party in the Complaint, and (2) the first-named party in each Cross-Complaint, if any.

Pursuant to Government Code section 70616(b), each party's complex case fee is due within ten (10) calendar days of this date.

Plaintiff shall serve a copy of this Order on all parties forthwith and file a proof of service within seven (7) days of service.

Any party objecting to the complex designation must file an objection and proof of service within ten (10) days of service of this Order. Any response to the objection must be filed within seven (7) days of service of the objection. The Court will make its ruling on the submitted pleadings.

The Case Management Conference remains set for **March 14, 2024 at 2:30 p.m. in Department 1** and all counsel are ordered to attend.

Counsel for all parties are ordered to meet and confer in person at least 15 days prior to the First Case Management Conference and discuss the following issues:

1. Issues related to recusal or disqualification;
2. Issues of law that, if considered by the Court, may simplify or further resolution of the case, including issues regarding choice of law;
3. Appropriate alternative dispute resolution (ADR), for example, mediation, mandatory settlement conference, arbitration, mini-trial;
4. A plan for preservation of evidence and a uniform system for identification of documents throughout the course of this litigation;
5. A plan for document disclosure/production and additional discovery; which will generally be conducted under court supervision and by court order;
6. Whether it is advisable to address discovery in phases so that information needed to conduct meaningful ADR is obtained early in the case (counsel should consider whether

they will stipulated to limited merits discovery in advance of certification proceedings), allowing the option to complete discovery if ADR efforts are unsuccessful;

7. Any issues involving the protection of evidence and confidentiality;
8. The handling of any potential publicity issues;

Counsel for Plaintiff is to take the lead in preparing a Joint Case Management Conference Statement to be filed 5 calendar days prior to the First Case Management Conference, and include the following:

1. a brief objective summary of the case;
2. a summary of any orders from prior case management conferences and the progress of the parties' compliance with said orders;
3. significant procedural and practical problems that may likely be encountered;
4. suggestions for efficient management, including a proposed timeline of key events; and
5. any other special consideration to assist the court in determining an effective case management plan.

To the extent the parties are unable to agree on the matters to be addressed in the Joint Case Management Conference Statement, the positions of each party or of various parties should be set forth separately and attached to this report as addenda. The parties are encouraged to propose, either jointly or separately, any approaches to case management they believe will promote the fair and efficient handling of this case. The Court is particularly interested in identifying potentially dispositive or significant threshold issues the early resolution of which may assist in moving the case toward effective ADR and/or a final disposition.


STAY ON DISCOVERY AND RESPONSIVE PLEADING DEADLINE Pending further order of this Court, the service of discovery and the obligation to respond to any outstanding discovery is stayed. However, Defendant(s) shall file a Notice of Appearance for purposes of identification of counsel and preparation of a service list. The filing of such a Notice of Appearance shall be without prejudice to the later filing of a motion to quash to contest jurisdiction. Parties shall not file or serve responsive pleadings, including answers to the complaint, motions to strike, demurrers, motions for change of venue and cross-complaints until a date is set at the First Case Management Conference for such filings and hearings.

This Order is issued to assist the Court and the parties in the management of this "Complex" case through the development of an orderly schedule for briefing and hearings. This Order shall not preclude the parties from continuing to informally exchange documents that may assist in their initial evaluation of the issues presented in this Case.

Plaintiff shall serve a copy of this Order on all the parties in this matter forthwith.

SO ORDERED.

Date: 11/15/2023



Hon. Sunil R. Kulkarni
Judge of the Superior Court

If you, a party represented by you, or a witness to be called on behalf of that party need an accommodation under the American with Disabilities Act, please contact the Court Administrator's office at (408) 882-2700, or use the Court's TDD line, (408) 882-2690 or the Voice/TDD California Relay Service, (800) 735-2922.

Exhibit C

RECEIVED

Judicial Council of California

JAN 24 2024

Coordination Lawyer

Mark N. Todzo (Bar No. 168389)
LEXINGTON LAW GROUP
503 Divisadero Street
San Francisco, CA 94117
Telephone: 415-913-7800
Facsimile: 415-759-4112
mtodzo@lexlawgroup.com

Attorneys for Petitioner

[Additional Counsel on Signature Page.]

JUDICIAL COUNCIL OF THE STATE OF CALIFORNIA

IN THE MATTER OF THE REQUEST FOR
COORDINATION OF THE FOLLOWING
ACTIONS:

IN THE SUPERIOR COURT FOR THE
COUNTY OF SAN FRANCISCO (Case No.
CGC-23-610816)

MARJORIE MORGENSTERN on Behalf of
Herself and All Others Similarly Situated,

Plaintiff,

v.

23ANDME HOLDING CO. and 23ANDME,
INC.,

Defendants.

IN THE SUPERIOR COURT FOR THE
COUNTY OF SANTA CLARA (Case No.
23CV424996):

KATHY VASQUEZ, Individually and on Behalf
of All Others Similarly Situated,

Plaintiff,

v.

23ANDME, INC.,

Defendant.

Judicial Counsel Coordination Proceeding
No. **5315**

**MEMORANDUM OF POINTS AND
AUTHORITIES IN SUPPORT OF
PETITION FOR COORDINATION**

[Filed concurrently with Petition for
Coordination; Declaration of Mark N.
Todzo; Application for Stay Order]

HEARING REQUESTED

TABLE OF CONTENTS

1			
2	INTRODUCTION.....		1
3	BACKGROUND.....		2
4	A. The 23andMe Data Breach.....		2
5	B. The <i>Morgenstern</i> Action		3
6	C. The <i>Vasquez</i> Action		3
7	ARGUMENT		3
8	A. Coordination of the Included Actions Subject to This Petition Is Appropriate		3
9	1. The Included Actions Are Complex.....		4
10	2. The Included Actions Present Common Questions of Fact and Law		
11	Which Are Significant and Predominating to the Litigation.....		5
12	3. Coordination Would Be Convenient for the Parties and Their Counsel		5
13	4. Coordination Would Result in the Efficient Utilization of Judicial		
14	Facilities and Manpower		6
15	5. Absent Coordination, Inconsistent Rulings in the Included Actions		
16	May Result in Inconsistent Regulation of the Sales of the Same		
17	Products		6
18	6. Coordination Will Promote Settlement in the Included Actions.....		6
19	B. The Included Actions Should Be Coordinated in San Francisco Superior		
20	Court.....		7
21	CONCLUSION		7
22			
23			
24			
25			
26			
27			
28			

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

PAGE(S)

CASES

Ford Motor Warranty Cases
11 Cal. App. 5th 626, 646 (2017)..... 4, 5

Keenan v. Sup. Ct.,
111 Cal. App. 3d 336 (1980)..... 4, 7

McGhan Med. Corp. v. Sup. Ct.,
11 Cal. App. 4th 804 (1992)..... 5

Pesses v. Sup. Ct.,
107 Cal. App. 3d 117 (1980)..... 4

STATUTES, RULES AND REGULATIONS

California Rules of Court
Rule 3.400 4
Rule 3.400(b)(1) 4
Rule 3.400(b)(2) 4
Rule 3.400(b)(3)
Rule 3.400(b)(4) 4
Rule 3.400(b)(5) 4
Rule 3.400(c)(6) 4
Rule 3.541(b)(2) 7

Cal. Civ. Code
§404 and C. 4
§404.1 3, 4, 6
§17983.100. 3

Cal. Bus. & Prof. Code
§17200 3

INTRODUCTION

This Petition seeks to coordinate actions pending in the Superior Courts of San Francisco and Santa Clara flowing from the massive data breach at 23andMe Holding Co. and 23andMe, Inc. (collectively, “23andMe”), which compromised the personal identifiable information (“PII”) and personal genetic and health information (“PGI”) of millions of customers. Dozens of actions have been filed against 23andMe in the Northern District of California’s San Francisco Division and other federal courts across the country and a motion to centralize those actions is currently pending before the Judicial Panel on Multidistrict Litigation.

23andMe is headquartered in San Francisco. Two actions against 23andMe are currently pending in California’s Superior Courts. In San Francisco Superior Court, Petitioner, Marjorie Morgenstern, filed *Morgenstern v. 23andMe Holding Co., et al.* (San Francisco Case No. 23-610816) (the “*Morgenstern* Action”). Ms. Morgenstern is represented by the Lexington Law Group, a San Francisco-based firm, and Scott+Scott Attorneys at Law LLP, an international class action firm with its primary office in New York. A separate action filed by Kathy Vasquez, *Vasquez v. 23andMe, Inc.*, (Santa Clara Case No. 23CV424996) (the “*Vasquez* Action”) is pending in Santa Clara, where 23andMe was previously headquartered. Ms. Vasquez is represented by attorneys near Los Angeles. The *Vasquez* Action has been designated as complex and is currently stayed.

Coordination of the *Morgenstern* and *Vasquez* Actions (collectively, the “Included Actions”) is both appropriate and necessary. These cases are complex, share the same basic underlying facts and legal theories, and raise identical issues. Given the near complete overlap in facts and legal theories, there is a substantial risk of inconsistent rulings, and the cases should accordingly be litigated in a single forum.

Petitioner seeks to have the Included Actions coordinated in San Francisco Superior Court. This is appropriate because 23andMe is headquartered in San Francisco and the relevant witnesses and their counsel are likely to be located in San Francisco. Further, the majority of the actions pending in federal court are pending in the Northern District of California’s San Francisco Division. Accordingly, the Included Actions should proceed in San Francisco, and this Petition should be heard by a San Francisco judge.

BACKGROUND

A. The 23andMe Data Breach

23andMe sells direct-to-consumer genetic testing kits to the public. To use 23andMe’s services, customers are required to provide a saliva sample that is subjected to single nucleotide polymorphism (“SNP”) genotyping. 23andMe identifies more than half a million SNPs from each saliva sample, which it uses to identify traits related to a person’s ancestry, wellness, health predispositions (including genetic health risks), and carrier status for inherited conditions. 23andMe claims to have more than 14 million customers.¹ According to 23andMe: “We receive and store a large volume of [personally identifiable information (“PII”) and personal genetic and health information (“PGI”)], and other data relating to our customers and patients. . . .”²

Though 23andMe was previously headquartered in Sunnyvale, California, as of April 1, 2022, the company relocated its corporate headquarters to South San Francisco, California, where it is currently based.³

On October 1, 2023, a hacker posted online a claim to have 23andMe users’ profile information. On October 6, 2023, 23andMe confirmed that “customer profile information” had been accessed “without the account users’ authorization,” and that a hacker had “obtained information from certain accounts, including information about users’ DNA Relatives profiles . . .” (the “Data Breach”).⁴ 23andMe has since stated that the information accessed by the hacker “generally included ancestry information, and, for a subset of those accounts, health-related information based upon the user’s genetics.”⁵ Posts on the dark web have purported to sell access to tens of millions of pieces of raw data exfiltrated from 23andMe.

¹ *23andMe for Healthcare Professionals*, 23ANDME (Nov. 3, 2023), <https://medical.23andme.com/> [<https://web.archive.org/web/20231030132819/https://medical.23andme.com/>].

² 23andMe Holding Co., Annual Report (Form 10-K) at 72 (March 31, 2022), <https://investors.23andme.com/static-files/536ba9a7-8a85-4b73-8b09-8215451089a0>.

³ *Id.*

⁴ *Addressing Data Security Concerns*, 23ANDME (Oct. 6, 2023; updated Dec. 5, 2023), <https://blog.23andme.com/articles/addressing-data-security-concerns> [<https://web.archive.org/web/20231007110808/>; <https://blog.23andme.com/articles/addressing-data-security-concerns>].

⁵ 23andMe Holding Co., Form 8-K/A, Am. 1 (Oct. 10, 2023).

B. The *Morgenstern* Action

Petitioner filed the *Morgenstern* Action on December 4, 2023, in San Francisco County Superior Court. Todzo Decl., Ex. 1. The *Morgenstern* Action asserts eight claims for relief against 23andMe, including for violations of California’s Unfair Competition Law, Cal. Bus. & Prof. Code §17200, California’s Consumer Privacy Act (“CCPA”), Cal. Civ. Code §17983.100, *et seq.*, and California’s Genetic Information Privacy Act (“GIPA”), Cal. Civ. Code §56.18, as well as claims for relief under the common law. *Id.*

Petitioner has duly served the operative Complaint and a summons on 23andMe. Todzo Decl., ¶5. Executed proofs of service were filed on January 9, 2024. *Id.* On December 15, 2023, Petitioner filed a Notice of Related Cases indicating the *Morgenstern* Action’s relation to cases pending in Federal Court in the Northern District of California. *Id.* On December 19, 2023, Petitioner filed an application to designate the *Morgenstern* Action as complex, which remains pending. An initial case management conference has been set for May 8, 2024. *Id.* Ms. Morgenstern served her initial set of written discovery requests on Defendants on January 19, 2024.

C. The *Vasquez* Action

Kathy Vasquez (“Vasquez”) filed the *Vasquez* Action on October 31, 2023, in Santa Clara Superior Court. Todzo Decl., ¶6. The *Vasquez* Action asserts seven claims for relief, most of which are also asserted in the *Morgenstern* Action. *Id.* On October 31, 2023, the Court set an initial case management conference for March 14, 2024. *Id.*, ¶8. While the summons was issued on October 31, 2023, no proof of service appears to have been filed. *Id.*, ¶7. On November 29, 2023, the Court entered an Order deeming the *Vasquez* Action complex and staying the discovery and responsive pleading deadline. *Id.*, ¶¶7-8.

ARGUMENT

A. Coordination of the Included Actions Subject to This Petition Is Appropriate

Coordination of complex civil actions sharing a common question of law or fact is appropriate if “one judge hearing all the actions for all purposes in a selected site or sites will promote the ends of justice.” C.C.P. §404.1. The factors for determining whether coordination will “promote the ends of justice” are: (1) whether the common question of fact or law is predominating

1 and significant to the litigation; (2) the convenience of parties, witnesses, and counsel; (3) the relative
 2 development of the actions and the work product of counsel; (4) the effective utilization of judicial
 3 resources; (5) the calendar of the courts; (6) the disadvantages of duplicative and inconsistent
 4 rulings, orders, or judgments; and (7) the likelihood of settlement of the actions without further
 5 litigation should coordination be denied. *Keenan v. Sup. Ct.*, 111 Cal. App. 3d 336, 341 (1980);
 6 *Pesses v. Sup. Ct.*, 107 Cal. App. 3d 117, 123 (1980).

7 Here, the Included Actions are plainly complex under C.R.C. Rule 3.400 and all of the C.C.P.
 8 §404.1 factors strongly favor coordination. As such, coordination of the Included Actions before a
 9 single judge would promote judicial efficiencies and the ends of justice.

10 **1. The Included Actions Are Complex**

11 The Included Actions, taken together, are complex within the meaning of C.C.P. §404 and
 12 C.R.C. Rule 3.400. *See Ford Motor Warranty Cases*, 11 Cal. App. 5th 626, 646 (2017). One of the
 13 Included Actions has already been ruled to meet the standards for complex cases pursuant to C.R.C.
 14 Rule 3.400, and the Included Actions as a whole are surely even more complex, not less. The
 15 Included Actions have been brought as class actions, which are inherently complex. C.R.C. Rule
 16 3.400(c)(6). Resolution of the Included Actions will require coordination to conserve judicial
 17 resources and ensure consistent results, including with regards to dispositive motions and motions
 18 for class certification. *See* C.R.C. Rule 3.400(b)(4). Given the scale of the Data Breach, involving
 19 millions of customers, and the sensitivity of the information compromised, there will likely be a
 20 large number of witnesses and substantial documentary evidence. *See* C.R.C. Rule 3.400(b)(2) &
 21 (3). Expert testimony will be required at class certification and trial to resolve various complex
 22 issues including regarding the types of data compromised, the vectors of compromise, and the types
 23 of security measures that would have been reasonable to implement under the circumstances. *See*
 24 C.R.C. Rule 3.400(b)(1). Finally, any consent judgments resolving these cases – which will likely
 25 require ongoing injunctive relief to prevent against any further data breaches – will require
 26 substantial post-judgment supervision. *See* C.R.C. Rule 3.400(b)(5). Thus, the Included Actions
 27 are complex.
 28

2. The Included Actions Present Common Questions of Fact and Law Which Are Significant and Predominating to the Litigation

The Included Actions share numerous common questions of law and fact which are significant and predominating. Common questions include whether 23andMe engaged in the misconduct alleged; whether 23andMe implemented and maintained data security measures that were inadequate to protect Plaintiffs and Class members' PII and PGI; whether 23andMe owed a duty to Plaintiffs and Class members and whether 23andMe breached that duty; whether 23andMe engaged in unfair or unlawful acts and practices; whether Petitioner and putative class members were injured and suffered damages as a result of 23andMe's conduct; and whether Petitioner and putative class members are entitled to relief and the measure of such relief.

Each of the Included Actions will require deduction of some of the same basic underlying facts and application of the same underlying law to those facts. The Included Actions each assert similar statutory and common law claims for relief making coordination appropriate. *See, e.g., McGhan Med. Corp. v. Sup. Ct.*, 11 Cal. App. 4th 804, 814 (1992) (coordination was proper where claims for relief, including negligence, were uniform across in several cases); *Ford Motor*, 11 Cal. App. 5th at 640 ("[A] great deal of efficiency can be accomplished by coordinating lemon law cases . . . despite individual issues relating to [auto] repair histories."). Since the Included Actions allege similar violations of law based on the same basic facts, those actions share predominating questions of fact and law and should be coordinated.

3. Coordination Would Be Convenient for the Parties and Their Counsel

A coordinated action would be more convenient for the parties and their counsel. 23andMe is headquartered in San Francisco, which is where most of the relevant witnesses are likely to be found. Counsel for Petitioner is also based in San Francisco, and the majority of the cases pending against 23andMe in Federal Court are in the Northern District of California's San Francisco division.

Given the overlapping issues raised by these cases, coordinated case management and briefing schedules will ensure that all parties are heard on matters that affect their substantive rights. Coordination of these cases would, for example, allow the court to schedule joint hearings on overlapping issues at the same time and even unrelated hearings on the same day. This would reduce litigation expenses for all parties and their attorneys.

As these cases are in their earliest phases, with discovery and the responsive pleading deadlines stayed in the *Vasquez* Action, Todzo Decl., ¶8, coordination makes particular sense at this juncture since the Coordination Trial Judge would be assigned the Included Actions before issuing substantive rulings.

4. Coordination Would Result in the Efficient Utilization of Judicial Facilities and Manpower

Coordination will promote judicial efficiency by requiring only one judge to become familiar with and rule on the novel legal questions and scientific issues at the heart of these cases. Data breach litigation involving class claims, such as the Included Actions, are inherently complex and expert intensive. Absent coordination, separate judges in separate courtrooms will be required to rule on the same legal and expert issues underlying these cases. By centralizing the Included Actions in a single court, a coordinated action will free up blocks of time on the calendar of the other court resulting in an overall reduction in time spent by the courts on these cases. Accordingly, “one judge hearing all of the actions for all purposes” would constitute an “efficient utilization of judicial facilities and manpower.” C.C.P. §404.1.

5. Absent Coordination, Inconsistent Rulings in the Included Actions May Result in Inconsistent Regulation of the Sales of the Same Products

Given the significant similarities of the Included Actions, inconsistent trial court rulings are highly likely if the cases are not coordinated. Absent coordination, different courts could come to opposite conclusions on identical questions, such as the duty of care owed to class members and whether 23andMe implemented and maintained data security measures that were inadequate to protect Plaintiffs and Class members’ PII and PGI. Separate rulings by different courts on the common issues raised by these cases could result in conflicting rulings regulating the exact same conduct. Coordination offers a means to avoid these unfortunate consequences.

6. Coordination Will Promote Settlement in the Included Actions

Coordination will significantly promote the final resolution of the claims raised in the Included Actions. Significantly, settlements reached in a coordinated proceeding following participation by both plaintiffs will provide the settling parties with certainty and finality.

B. The Included Actions Should Be Coordinated in San Francisco Superior Court

Under the coordination rules, the Coordination Motion Judge determines the appropriate venue based on many of the same factors used to approve the coordination in the first instance: the convenience of the parties, witnesses, and counsel; the relative development of the actions; the efficient utilization of judicial facilities; and the calendar of the courts. C.R.C. Rule 3.541(b)(2); *see also Keenan*, 111 Cal. App. 3d at 342. Applying those criteria to the cases at hand, Petitioner respectfully recommends coordination of the cases in the County of San Francisco.

Venue in San Francisco County will be convenient for the parties, witnesses, and counsel. 23andMe is headquartered in San Francisco, which is where most of the relevant witnesses are likely to be found. Counsel for Petitioner is also based in San Francisco, and the majority of the cases pending against 23andMe in Federal Court are in the Northern District of California's San Francisco division. As no active litigation has yet taken place in the *Vasquez* Action, the parties will not be prejudiced by a transfer of the *Vasquez* Action to San Francisco County at this early stage in the litigation.

CONCLUSION

For the foregoing reasons, Petitioner respectfully request that its Petition for Coordination be granted.

Dated: January 24, 2024

LEXINGTON LAW GROUP



Mark N. Todzo (Bar No. 168389)
Patrick R. Carey (Bar No. 308623)
Meredyth L. Merrow (Bar No. 328337)
503 Divisadero Street
San Francisco, CA 94117

Joseph P. Guglielmo (*pro hac vice* forthcoming)
Carey Alexander (*pro hac vice* forthcoming)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169-1820
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com

Attorneys for Petitioner

Exhibit D

RECEIVED

Judicial Council of California

JAN 24 2024

Eric Dilworth (v.a.)
Coordination Lawyer

1 Mark N. Todzo (Bar No. 168389)
2 **LEXINGTON LAW GROUP**
3 503 Divisadero Street
4 San Francisco, CA 94117
5 Telephone: 415-913-7800
6 Facsimile: 415-759-4112
7 mtodzo@lexlawgroup.com

8 *Attorneys for Petitioner*

9 [Additional Counsel on Signature Page.]

10 **JUDICIAL COUNCIL OF THE STATE OF CALIFORNIA**

11 IN THE MATTER OF THE REQUEST FOR
12 COORDINATION OF THE FOLLOWING
13 ACTIONS:

14 IN THE SUPERIOR COURT FOR THE
15 COUNTY OF SAN FRANCISCO (Case No.
16 CGC-23-610816)

17 MARJORIE MORGENSTERN on Behalf of
18 Herself and All Others Similarly Situated,

19 Plaintiff,

20 v.

21 23ANDME HOLDING CO. and 23ANDME,
22 INC.,

23 Defendants.

24 IN THE SUPERIOR COURT FOR THE
25 COUNTY OF SANTA CLARA (Case No.
26 23CV424996):

27 KATHY VASQUEZ, Individually and on Behalf
28 of All Others Similarly Situated,

Plaintiff,

v.

23ANDME, INC.,

Defendant.

Judicial Counsel Coordination
Proceeding No. **5315**

APPLICATION FOR STAY ORDER

[Filed concurrently with Petition for
Coordination; Memorandum of Points and
Authorities, Declaration of Mark N.
Todzo]

HEARING REQUESTED

1 In connection with the Petition for Coordination (the “Petition”) filed herewith, and
 2 pursuant to Code of Civil Procedure (“C.C.P.”) § 404.5 and the California Rules of Court
 3 (“C.R.C.”), Petitioner Marjorie Morgenstern (“Petitioner”) hereby makes an application for an
 4 order staying the action brought by Kathy Vasquez (“*Vasquez*”) identified below, pending a
 5 determination of whether the actions shall be coordinated.

6 The complete title and case number of each case known by Petitioner to be a related case
 7 pending in a court of the State of California that is subject to coordination (“Included Actions”), the
 8 court in which such case is pending, and the filing date of each, are as follows:

9 1. Marjorie Morgenstern, on behalf of herself and all others similarly situated,

10
 11 Plaintiff,

12 v.

13 23andMe Holding Co. and 23andMe, Inc.

14 Defendants.

15 San Francisco County Superior Court, Case No. CGC-23-610816, filed December 4,
 16 2023 (the “*Morgenstern* Action”);

17 2. Kathy Vasquez,

18 Plaintiff,

19 v.

20 23andMe, Inc.

21 Defendant.

22 Santa Clara County Superior Court, Case No. 23CV424996, filed October 31, 2023 (the
 23 “*Vasquez* Action”);

24
 25 The judge determining whether coordination is appropriate may stay any included action to
 26 effectuate the purposes of coordination. C.C.P. § 404.5; C.R.C. Rule 3.515. Here, preserving the
 27 status quo in the above-referenced *Vasquez* Action is necessary to effectuate the purposes of
 28 coordination: to ensure consistent results, preserve judicial resources, and provide each affected

1 party an opportunity to be heard before its substantive rights are affected. Although the *Vasquez*
 2 Action is currently stayed as to discovery and responsive pleading deadlines, Petitioner wants to
 3 ensure the case is stayed during the entire pendency of the coordination petition. Todzo Decl., Exh.
 4 3. The status of the *Vasquez* Action demonstrates the parties will not be prejudiced by an order to
 5 stay.

6 Additionally, the Included Actions raise nearly identical claims of relief. *See* Todzo Decl.,
 7 ¶4-8. Thus, there is a risk that, absent a stay, the Santa Clara judge overseeing the *Vasquez* Action
 8 could issue a ruling that conflicts with the proceeding in San Francisco County. Accordingly, a
 9 stay of the *Vasquez* Action is appropriate. *See* C.R.C. Rule 3.515(f) (stay should be granted where
 10 “a final judgment in [the] action [proposed to be coordinated] would have a res judicata or
 11 collateral estoppel effect with regard to any common issue of the included actions”).

12 The facts relied upon by Petitioner to show that a stay order is necessary and appropriate to
 13 effectuate the purposes of coordination are set forth in more detail in the accompanying Declaration
 14 of Mark N. Todzo and Memorandum of Points and Authorities in Support of Petition for
 15 Coordination, made a part of this Application by reference as if fully set forth herein. Petitioner
 16 respectfully requests a hearing on this Application.

17
 18 Dated: January 24, 2024

LEXINGTON LAW GROUP



 Mark N. Todzo (Bar No. 168389)
 Patrick R. Carey (Bar No. 308623)
 Meredyth L. Merrow (Bar No. 328337)
 503 Divisadero Street
 San Francisco, CA 94117

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Joseph P. Guglielmo (*pro hac vice* forthcoming)
Carey Alexander (*pro hac vice* forthcoming)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169-1820
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com

Attorneys for Petitioner

Exhibit F

Electronically Filed
by Superior Court of CA,
County of Santa Clara,
on 3/5/2024 12:17 PM
Reviewed By: R. Walker
Case #23CV424996
Envelope: 14603134

SUPERIOR COURT OF CALIFORNIA
COUNTY OF SANTA CLARA

Coordination Proceeding
Special Title (Rule 3.550)

23ANDME DATA BREACH CASES

JUDICIAL COUNCIL
COORDINATION PROCEEDING
NO. 5315¹

**ORDER ASSIGNING
COORDINATION MOTION JUDGE**

THE **HONORABLE CHARLES F. ADAMS**, Judge of the Superior Court, County of Santa Clara, is hereby assigned pursuant to Code of Civil Procedure Section 404 and Rule 3.524, California Rules of Court, to sit as coordination **motion** judge to determine whether the actions are complex (Rule 3.502), and if so, whether coordination of the included actions listed below is appropriate. If the coordination motion judge grants the petition for coordination, the coordination motion judge shall also (1) recommend a particular superior court for the site of

¹ Included Actions: (1) Morgenstern v. 23ANDME Holding Co., et al., Superior Court of California, County of San Francisco, Case No. CGC-23-610816; (2) Vasquez v. 23ANDME, Inc., Superior Court of California, County of Santa Clara, Case No. 23CV424996.

the coordination proceedings, pursuant to Rule 3.530, and (2) select the reviewing court having appellate jurisdiction if the actions to be coordinated are within the jurisdiction of more than one reviewing court, pursuant to Rule 3.505(a).

Pursuant to Code of Civil Procedure section 404.5 and Rule 3.515, pending any determination whether coordination is appropriate, the coordination motion judge may stay any action being considered for, or affecting an action being considered for, coordination.

INCLUDED ACTIONS

<u>COURT</u>	<u>NUMBER</u>	<u>SHORT TITLE</u>
Superior Court of California County of San Francisco	CGC-23-610816	Morgenstern v. 23ANDME Holding Co., et al.
Superior Court of California County of Santa Clara	23CV424996	Vasquez v. 23ANDME, Inc.

Pursuant to Rule 3.524, the clerk of each court in which an included action is pending is directed to file this order in the included action. Also pursuant to Rule 3.524, all documents required to be submitted to the coordination motion judge shall be submitted to him at the court address designated below.

Hon. Charles F. Adams
Superior Court of California
County of Santa Clara, Department 7
191 North First Street
San Jose, CA 95113

Pursuant to Rule 3.511, a copy of every notice of opposition, application for stay order, stay order, notice of hearing on the petition, and order granting or denying coordination must be transmitted to the Chair of the Judicial Council at the following address:

1 Chair, Judicial Council of California
2 Administrative Office of the Courts
3 Attn: Office of Appellate Court Services
4 (Civil Case Coordination)
5 455 Golden Gate Avenue, 5th Floor
6 San Francisco, CA 94102-3688

7 Petitioner is directed to serve a copy of this order on (1) all parties to the included
8 actions, and (2) the clerk of each court for filing in each included action.

9 SO ORDERED.

10 Dated: 3/5/24


11 
12 Honorable Beth McGowan
13 Presiding Judge of the Superior Court
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Exhibit G

GREENBERG TRAURIG, LLP
Ian C. Ballon (SBN 141819)
Ballon@gtlaw.com
1900 University Avenue, 5th Floor
East Palo Alto, California 94303
Telephone: 650-328-8500

Rebekah S. Guyon (SBN 291037)
GuyonR@gtlaw.com
Adam M. Korn (SBN 333270)
Adam.Korn@gtlaw.com
1840 Century Park East, Suite 1900
Los Angeles, California 90067
Telephone: 310-586-7700

Kristin O'Carroll (SBN 312902)
ocarrollk@gtlaw.com
101 Second Street, Suite 2200
San Francisco, California 94105-3668
Telephone: 415-655-1300

Attorneys for Defendant 23andMe, Inc.

**Electronically Filed
by Superior Court of CA,
County of Santa Clara,
on 6/7/2024 4:41 PM
Reviewed By: R. Walker
Case #23CV424996
Envelope: 15580676**

**SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SANTA CLARA**

Coordination Proceeding
Special Title (Rule 3.550)

JUDICIAL COUNCIL COORDINATION
PROCEEDING NO. 5315

Underlying Case No. 24-cv-429673

23ANDME DATA BREACH CASES

**DEFENDANT 23ANDME, INC'S NOTICE
OF POTENTIAL ADD-ON CASE**

PLEASE TAKE NOTICE that pursuant to California Rule of Court, rule 3.531, Defendant 23andMe, Inc. (“23andMe”) in the action *Wilkus v. 23andMe, Inc.* Case No. 24-cv-429673 (“*Wilkus*”) hereby notifies the Court and the Chair of the Judicial Council of the pendency of an additional action in the State of California, Santa Clara County, that is related to the pending coordination proceedings before this Court in the above-captioned proceedings (“23andMe Data Breach Cases,” Judicial Council Coordination Proceeding No. 5315), which seeks to coordinate the following actions:

- *Morgenstern v. 23andMe Holding Co., et al.* (San Francisco Case No. 23-610816) (“*Morgenstern*”)
- *Vasquez v. 23andMe, Inc.*, (Santa Clara Case No. 23CV424996) (“*Vasquez*”)

Wilkus was filed on January 23, 2024—two days before the filing of the initial Petition for Coordination in these proceedings (the “Petition”). 23andMe hereby requests that the Court enter an order adding *Wilkus* to the Petition for Coordination in JCCP No. 5315. *Wilkus* should be coordinated with the *Morgenstern* and *Vasquez* actions included in the Petition because substantially similar legal issues and factual allegations predominate all three cases. The potential add-on case states claims for (1) Violation of the Illinois Genetic Information Privacy Act, 410 Ill. Comp. Stat. Ann. 513 *et seq.*, (“GIPA”) (2) Negligence, (3) Breach of Actual and Implied Contract, (4) Invasion of Privacy—Intrusion Upon Seclusion, and (5) Unjust Enrichment. *See* Ex. A [*Wilkus* Complaint]. These claims arise from an alleged security incident in which unauthorized actors managed to access certain user accounts through a credential stuffing attack on a narrow subset of accounts that used compromised login credentials. *Id.* Using this access, an unauthorized third party was able to access profile information that certain 23andMe users had shared with up to millions of other individuals on the platform via the optional DNA Relatives or Family Tree features of 23andMe (the “Incident”). Each of the actions included in the Petition also arises from the Incident—an alleged “exposure of Petitioner’s personal identifiable information (“PII”) and personal genetic and health information (“PGI”)”. *See* Ex. B at ¶6 [Petition]. Plaintiffs in *Wilkus* are members of the putative classes that plaintiffs seek to represent in the actions included in the Petition.

Wilkus is subject to coordination because it is complex within the meaning of section 404 of the California Code of Civil Procedure. “Only cases that are ‘complex’ as defined by the Judicial Council standards may be coordinated.” *See* Weil & Brown, Cal. Practice Guide: Civ. Pro. Before Trial (The Rutter

Group June 2023 Update) ¶ 12:374.5). A “complex case” is defined as “an action that requires exceptional judicial management to avoid placing unnecessary burdens on the court or the litigants and to expedite the case, keep costs reasonable, and promote effective decision making by the court, the parties, and counsel.” See CRC rule 3.400(a). A complex case includes a matter that will require “[c]oordination with related actions pending in one or more courts in other counties, states, or countries, or in a federal court.” CRC rule 3.400(b)(4). Here, in addition to the three state court cases at issue, forty (40) lawsuits have been filed in federal courts around the country in which plaintiffs assert claims allegedly arising from the Incident, and the overlapping litigation—including overlapping putative class definitions and putative classes that include the *Wilkus* plaintiffs—will require coordination amongst the parties. Most of the federal cases were filed in the Northern District of California; however, three cases were filed outside of the Northern District of California, one in the Northern District of Illinois, one in California state court (which 23andMe subsequently removed to the Central District of California), and one in Illinois state court (which 23andMe subsequently removed to the Northern District of Illinois). On April 12, 2024, the Judicial Panel on Multidistrict Litigation (“JPML”) ordered transfer and coordination of the federal cases to the Northern District of California, where they are currently pending in front of Judge Edward M. Chen.

Moreover, in the absence of overlapping claims in federal court, *Wilkus* should be coordinated with the actions subject to the Petition because, as stated above, the *Wilkus* plaintiffs are members of the putative classes that plaintiffs in the cases subject to the Petition seek to represent.

Finally, although 23andMe denies that any plaintiffs’ claims have merit, *Wilkus* is also complex under the California Rules of Court because it is likely to involve “novel legal issues that will be time-consuming to resolve” in light of the factual scenario underlying plaintiffs’ claims and because GIPA, under which plaintiffs sue, was relatively recently enacted. CRC rule 3.400(b)(1). Thus, coordination of this complex case with the actions subject to the Petition is appropriate.

Therefore, 23andMe hereby requests that the Coordination Motion Judge issue an order deeming the potential add-on case as an Included Action for the purposes of the hearing on the pending Petition.

Further, pursuant to sections 404.4 and 404.5 of the California Code of Civil Procedure, 23andMe requests *Wilkus* be ordered stayed, except for proceedings relating to coordination, until such time as the Coordination Judge orders otherwise.

1 Proof of filing in *Wilkus* of this Notice of Potential Add-On and a copy of the accompanying
2 proposed order, pursuant to Rule 3.522 of the California Rules of Court will be submitted to the Chair of
3 the Judicial Council and the Coordination Motion Judge.

4 Submitted contemporaneously with this notice is a proposed order for consideration by the
5 Coordination Motion Judge to deem the potential add-on case identified above as an Included Action for
6 purposes of JCCP No. 5315.

7
8 DATED: June 7, 2024

GREENBERG TRAURIG, LLP

9
10 By: /s/ Rebekah S. Guyon
11 Rebekah S. Guyon
12 Attorneys for Defendant 23andMe, Inc.
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PROOF OF SERVICE**STATE OF CALIFORNIA, COUNTY OF LOS ANGELES**

I am employed in the aforesaid county, State of California; I am over the age of 18 years and not a party to the within action; my business address is 1840 Century Park East, 19th Floor, Los Angeles, CA 90067, email sharifh@gtlaw.com.

On the date given below, I served the **DEFENDANT 23ANDME, INC'S NOTICE OF POTENTIAL ADD-ON CASE** on the interested parties in this action addressed as follows:

SEE ATTACHED SERVICE LIST☒ **(BY FIRST CLASS MAIL)**

I am readily familiar with the business practice of my place of employment in respect to the collection and processing of correspondence, pleadings and notices for mailing with United States Postal Service. The foregoing sealed envelope was placed for collection and mailing this date consistent with the ordinary business practice of my place of employment, so that it will be picked up this date with postage thereon fully prepaid at Los Angeles, California, in the ordinary course of such business.

☒ **(BY E-MAIL)** I caused the above document(s) to be transmitted to the office(s) of the addressee(s) listed above by electronic mail at the e-mail address(es) set forth above per agreement and consent of the addressee(s). The document was served electronically and the transmission was reported complete and without error.☐ **(BY OVERNIGHT DELIVERY)**

I enclosed the documents in an envelope or package provided by an overnight delivery carrier and addressed to the persons above. I placed the envelope or package for collection and overnight delivery at an office or a regularly utilized drop box of the overnight delivery carrier.

☐ **(BY PERSONAL SERVICE)**

I caused such envelope to be delivered by hand to the offices listed above.

☒ **(STATE)** I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on June 7, 2024, at Los Angeles, California.



Haleh Sharifi

SERVICE LIST

Jason M. Wucetich
Dimitrios V. Korovilas
Wucetich & Korovilas LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, California 90245
Tel. (310) 335-2001
Fax (310) 364-5201
Jason@Wukolaw.com
Dimitri@Wukolaw.com
Attorneys for Plaintiff Kathy Vasquez

Mark N. Todzo
Lexington Law Group
503 Divisadero Street
San Francisco, CA 94117
Telephone: 415-913-7800
Facsimile: 415-759-4112
mtodzo@lexlawgroup.com
Joseph P. Guglielmo
Carey Alexander
Scott+Scott Attorneys At Law LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169-1820
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com
Attorneys for Plaintiff Marjorie Morgenstern

Mark Potter, Esq.,
Barry Walker, Esq.,
Jim Treglio, Esq.,
Christina Carson, Esq.
Tehniat Zaman, Esq.
Potter Handy, LLP
Mail: 100 Pine St., Ste. 1250
San Francisco, CA 94111
(415) 534-1911; (888) 422-5191
BarryW@potterhandy.com
mark@potterhandy.com
jimt@potterhandy.com;
ChrisC@potterhandy.com
tehnitz@potterhandy.com

1 *Attorneys for Plaintiffs Trisha Wilkus; Ryan Fowler; Arturo Gonzalez; Sarah Schultz; Cassandra*
2 *Salgado; Melanie DiMuzio; Darlene Eby; Sandy Landvick; Dalia Ramahi; Patty Zink; Katharina*
3 *Ryasati; Steve Temkin; and Nicole Cassidy,*

4 Judicial Council of California
5 455 Golden Gate Avenue,
6 San Francisco, CA 94102-3688.
7 Email: coordination@jud.ca.gov
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

GREENBERG TRAURIG, LLP
Ian C. Ballon (SBN 141819)
Ballon@gtlaw.com
1900 University Avenue, 5th Floor
East Palo Alto, California 94303
Telephone: 650-328-8500

Rebekah S. Guyon (SBN 291037)
GuyonR@gtlaw.com
Adam M. Korn (SBN 333270)
Adam.Korn@gtlaw.com
1840 Century Park East, Suite 1900
Los Angeles, California 90067
Telephone: 310-586-7700

Kristin O'Carroll (SBN 312902)
ocarrollk@gtlaw.com
101 Second Street, Suite 2200
San Francisco, California 94105-3668
Telephone: 415-655-1300

Attorneys for Defendant 23andMe, Inc.

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SANTA CLARA

Coordination Proceeding
Special Title (Rule 3.550)

JUDICIAL COUNCIL COORDINATION
PROCEEDING NO. 5315

Underlying Case No. TC24-2263

23ANDME DATA BREACH CASES

**DEFENDANT 23ANDME, INC'S NOTICE
OF POTENTIAL ADD-ON CASE**

PLEASE TAKE NOTICE that pursuant to California Rule of Court, rule 3.531, Defendant 23andMe, Inc. (“23andMe”) in the action *Shaw v. 23andMe, Inc.* Case No. TC24-2263 (“*Shaw*”) hereby notifies the Court and the Chair of the Judicial Council of the pendency of an additional action in the State of California, Santa Clara County, that is related to the pending coordination proceedings before this Court in the above-captioned proceedings (“23andMe Data Breach Cases,” Judicial Council Coordination Proceeding No. 5315), which seeks to coordinate the following actions:

- *Morgenstern v. 23andMe Holding Co., et al.* (San Francisco Case No. 23-610816) (“*Morgenstern*”)
- *Vasquez v. 23andMe, Inc.*, (Santa Clara Case No. 23CV424996) (“*Vasquez*”)
- *Wilkus v. 23andMe, Inc.* (Santa Clara Case No. 24-cv-429673) (“*Wilkus*”)

Shaw was filed on July 9, 2024—nearly seven months after the filing of the initial Petition for Coordination in these proceedings (the “Petition”). 23andMe hereby requests that the Court enter an order adding *Shaw* to the Petition for Coordination in JCCP No. 5315. *Shaw* should be coordinated with the *Morgenstern*, *Wilkus*, and *Vasquez* actions included in the Petition because substantially similar legal issues and factual allegations predominate all three cases. In fact, the *Shaw* complaint is a verbatim duplicate of the *Wilkus* complaint. *Wilkus* and *Shaw* both case states claims for (1) Violation of the Illinois Genetic Information Privacy Act, 410 Ill. Comp. Stat. Ann. 513 *et seq.*, (“GIPA”) (2) Negligence, (3) Breach of Actual and Implied Contract, (4) Invasion of Privacy—Intrusion Upon Seclusion, and (5) Unjust Enrichment. *See* Ex. A [*Shaw* Complaint]; Ex. B [*Wilkus* Complaint]. These claims arise from an alleged security incident in which unauthorized actors managed to access certain user accounts through a credential stuffing attack on a narrow subset of accounts that used compromised login credentials. *Id.* Using this access, an unauthorized third party was able to access profile information that certain 23andMe users had shared with up to millions of other individuals on the platform via the optional DNA Relatives or Family Tree features of 23andMe (the “Incident”). Each of the actions included in the Petition also arises from the Incident—an alleged “exposure of Petitioner’s personal identifiable information (“PII”) and personal genetic and health information (“PGI”)”. *See* Ex. C at ¶6 [Petition]. Plaintiffs in *Shaw*, like Plaintiffs in *Wilkus*, are members of the putative classes that plaintiffs seek to represent in the actions included in the Petition.

1 *Shaw* is subject to coordination because it is complex within the meaning of section 404 of the
2 California Code of Civil Procedure. “Only cases that are ‘complex’ as defined by the Judicial Council
3 standards may be coordinated.” *See* Weil & Brown, Cal. Practice Guide: Civ. Pro. Before Trial (The Rutter
4 Group June 2023 Update) ¶ 12:374.5). A “complex case” is defined as “an action that requires exceptional
5 judicial management to avoid placing unnecessary burdens on the court or the litigants and to expedite the
6 case, keep costs reasonable, and promote effective decision making by the court, the parties, and counsel.”
7 *See* CRC rule 3.400(a). A complex case includes a matter that will require “[c]oordination with related
8 actions pending in one or more courts in other counties, states, or countries, or in a federal court.” CRC
9 rule 3.400(b)(4). Here, in addition to the three state court cases at issue, forty (40) lawsuits have been filed
10 in federal courts around the country in which plaintiffs assert claims allegedly arising from the Incident,
11 and the overlapping litigation—including overlapping putative class definitions and putative classes that
12 include the *Shaw* plaintiffs—will require coordination amongst the parties. Most of the federal cases were
13 filed in the Northern District of California; however, three cases were filed outside of the Northern District
14 of California, one in the Northern District of Illinois, one in California state court (which 23andMe
15 subsequently removed to the Central District of California), and one in Illinois state court (which 23andMe
16 subsequently removed to the Northern District of Illinois). On April 12, 2024, the Judicial Panel on
17 Multidistrict Litigation (“JPML”) ordered transfer and coordination of the federal cases to the Northern
18 District of California, where they are currently pending in front of Judge Edward M. Chen.

19 Moreover, in the absence of overlapping claims in federal court, *Shaw* should be coordinated with
20 the actions subject to the Petition because, as stated above, the *Shaw* plaintiffs are members of the putative
21 classes that plaintiffs in the cases subject to the Petition seek to represent.

22 Finally, although 23andMe denies that any plaintiffs’ claims have merit, *Shaw* is also complex
23 under the California Rules of Court because it is likely to involve “novel legal issues that will be time-
24 consuming to resolve” in light of the factual scenario underlying plaintiffs’ claims and because GIPA,
25 under which plaintiffs sue, was relatively recently enacted. CRC rule 3.400(b)(1). Thus, coordination of
26 this complex case with the actions subject to the Petition is appropriate.

27 Therefore, 23andMe hereby requests that the Coordination Motion Judge issue an order deeming
28 the potential add-on case as an Included Action for the purposes of the hearing on the pending Petition.

1 Further, pursuant to sections 404.4 and 404.5 of the California Code of Civil Procedure, 23andMe
2 requests *Shaw* be ordered stayed, except for proceedings relating to coordination, until such time as the
3 Coordination Judge orders otherwise.

4 Proof of filing in *Shaw* of this Notice of Potential Add-On and a copy of the accompanying proposed
5 order, pursuant to Rule 3.522 of the California Rules of Court will be submitted to the Chair of the Judicial
6 Council and the Coordination Motion Judge.

7 Submitted contemporaneously with this notice is a proposed order for consideration by the
8 Coordination Motion Judge to deem the potential add-on case identified above as an Included Action for
9 purposes of JCCP No. 5315.

10
11 DATED: July 12, 2024

GREENBERG TRAURIG, LLP

12
13 By: /s/ Rebekah S. Guyon
14 Rebekah S. Guyon
15 Attorneys for Defendant 23andMe, Inc.
16
17
18
19
20
21
22
23
24
25
26
27
28

Exhibit H

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SANTA CLARA

191 N. FIRST STREET
SAN JOSE, CA 95113-1090

**Electronically Filed
by Superior Court of CA,
County of Santa Clara,
on 6/10/2024 10:11 AM
Reviewed By: R. Walker
Case #24CV429673
Envelope: 15587157**

TO: FILE COPY

RE: Vasquez v. 23ANDME, Inc.
CASE NUMBER: 23CV424996

RE: Wilkus, et al. v. 23andMe, Inc.
CASE NUMBER: 24CV429673

ORDER AND NOTICE OF REASSIGNMENT OF CASES

A review of the above-entitled actions has determined that these actions are related within the meaning of California Rules of Court Rule 3.300. The Court has determined that the actions involve some of the same parties, are based on the same or similar claims, and involve the same transaction or events.

Accordingly, the assignment of the matters to the same judge is likely to effect a substantial savings of judicial effort and is also likely to be convenient to the parties.

The parties are notified that relating the cases under California Rules of Court Rule 3.300 merely has the result that these three matters are assigned to the same judge; no consolidation of the actions has been ordered.

The earlier filed case, Vasquez, Case No. 23CV424996, is currently assigned to Department 7, the Hon. Charles F. Adams presiding; this matter is also included in *23ANDME Data Breach Cases*, Judicial Council Proceeding Case No. 5315. The later filed case, Wilkus, Case No. 24CV429673, is currently assigned to Department 16, the Hon. Amber Rosen presiding; the request for determination of Wilkus as an included action in JCCP5315 is pending with the Court.

IT IS THEREFORE ORDERED THAT Case No. 24CV429673 be, and is, reassigned to **Department 7**, the **Hon. Charles F. Adams** presiding, for all purposes, including discovery, law & motion, settlement conference, and trial. Any and all hearing dates set before Department 16 in Case No. 24CV429673 are now vacated. The Case Management Conference is rescheduled from July 9, 2024 to July 18, 2024 at 2:30 p.m. in Department 7.

The two cases referenced above are ordered related.

///

///

///

Please contact the Complex Civil Litigation Department, (408) 882-2286 or rwalker@scscourt.org, if you have any questions.

SO ORDERED.

Date Issued: June 10, 2024



Hon. Evette D. Pennypacker
Civil Supervising Judge
Judge of the Superior Court

If you, a party represented by you, or a witness to be called on behalf of that party need an accommodation under the American with Disabilities Act, please contact the Court Administrator's office at (408) 882-2700, or use the Court's TDD line, (408) 882-2690 or the Voice/TDD California Relay Service, (800) 735-2922.

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SANTA CLARA

191 N. FIRST STREET
SAN JOSE, CA 95113-1090

Electronically Filed
by Superior Court of CA,
County of Santa Clara,
on 6/11/2024 12:19 PM
Reviewed By: R. Walker
Case #24CV429673
Envelope: 15604775

TO: FILE COPY

RE: Wilkus, et al. v. 23andMe, Inc.
CASE NUMBER: **24CV429673**

**ORDER DEEMING CASE COMPLEX AND STAYING DISCOVERY
AND RESPONSIVE PLEADING DEADLINE**

WHEREAS, the Complaint was filed by Plaintiffs **Trisha Wilkus** ("Plaintiff"), et al. in the Superior Court of California, County of Santa Clara, on **January 23, 2024** and reassigned on or about June 10, 2024 to Department **7** (Complex Civil Litigation), the **Honorable Charles F. Adams** presiding, pending a ruling on the complexity issue;

IT IS HEREBY ORDERED that:

The Court determines that the above-referenced case is **COMPLEX** within the meaning of California Rules of Court 3.400. The matter remains assigned, for all purposes, including discovery and trial, to Department **7** (Complex Civil Litigation), the **Honorable Charles F. Adams** presiding.

The parties are directed to the Court's local rules and guidelines regarding electronic filing and to the Complex Civil Guidelines, which are available on the Court's website.

Pursuant to California Rules of Court, Rule 3.254, the creation and maintenance of the Master Service List shall be under the auspices of (1) Plaintiff **Trisha Wilkus**, as the first-named party in the Complaint, and (2) the first-named party in each Cross-Complaint, if any.

Pursuant to Government Code section 70616(b), each party's complex case fee is due within ten (10) calendar days of this date.

Plaintiff shall serve a copy of this Order on all parties forthwith and file a proof of service within seven (7) days of service.

Any party objecting to the complex designation must file an objection and proof of service within ten (10) days of service of this Order. Any response to the objection must be filed within seven (7) days of service of the objection. The Court will make its ruling on the submitted pleadings.

The Case Management Conference remains set for **July 18, 2024 at 2:30 p.m. in Department 7** and all counsel are ordered to attend.

Counsel for all parties are ordered to meet and confer in person at least 15 days prior to the First Case Management Conference and discuss the following issues:

1. Issues related to recusal or disqualification;
2. Issues of law that, if considered by the Court, may simplify or further resolution of the case, including issues regarding choice of law;
3. Appropriate alternative dispute resolution (ADR), for example, mediation, mandatory settlement conference, arbitration, mini-trial;
4. A plan for preservation of evidence and a uniform system for identification of documents throughout the course of this litigation;
5. A plan for document disclosure/production and additional discovery; which will generally be conducted under court supervision and by court order;

6. Whether it is advisable to address discovery in phases so that information needed to conduct meaningful ADR is obtained early in the case (counsel should consider whether they will stipulated to limited merits discovery in advance of certification proceedings), allowing the option to complete discovery if ADR efforts are unsuccessful;
7. Any issues involving the protection of evidence and confidentiality;
8. The handling of any potential publicity issues;

Counsel for Plaintiff is to take the lead in preparing a Joint Case Management Conference Statement to be filed 5 calendar days prior to the First Case Management Conference, and include the following:

1. a brief objective summary of the case;
2. a summary of any orders from prior case management conferences and the progress of the parties' compliance with said orders;
3. significant procedural and practical problems that may likely be encountered;
4. suggestions for efficient management, including a proposed timeline of key events; and
5. any other special consideration to assist the court in determining an effective case management plan.

To the extent the parties are unable to agree on the matters to be addressed in the Joint Case Management Conference Statement, the positions of each party or of various parties should be set forth separately and attached to this report as addenda. The parties are encouraged to propose, either jointly or separately, any approaches to case management they believe will promote the fair and efficient handling of this case. The Court is particularly interested in identifying potentially dispositive or significant threshold issues the early resolution of which may assist in moving the case toward effective ADR and/or a final disposition.

STAY ON DISCOVERY AND RESPONSIVE PLEADING DEADLINE Pending further order of this Court, the service of discovery and the obligation to respond to any outstanding discovery is stayed. However, Defendant(s) shall file a Notice of Appearance for purposes of identification of counsel and preparation of a service list. The filing of such a Notice of Appearance shall be without prejudice to the later filing of a motion to quash to contest jurisdiction. Parties shall not file or serve responsive pleadings, including answers to the complaint, motions to strike, demurrers, motions for change of venue and cross-complaints until a date is set at the First Case Management Conference for such filings and hearings.

This Order is issued to assist the Court and the parties in the management of this "Complex" case through the development of an orderly schedule for briefing and hearings. This Order shall not preclude the parties from continuing to informally exchange documents that may assist in their initial evaluation of the issues presented in this Case.

Plaintiff shall serve a copy of this Order on all the parties in this matter forthwith.

SO ORDERED.

Date: 6/10/2024 9:17:41 PM



Hon. Charles F. Adams
Judge of the Superior Court

If you, a party represented by you, or a witness to be called on behalf of that party need an accommodation under the American with Disabilities Act, please contact the Court Administrator's office at (408) 882-2700, or use the Court's TDD line, (408) 882-2690 or the Voice/TDD California Relay Service, (800) 735-2922.

Exhibit I

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SANTA CLARA

**191 N. FIRST STREET
SAN JOSE, CA 95113-1090**

**Electronically Filed
by Superior Court of CA,
County of Santa Clara,
on 7/12/2024 10:25 AM
Reviewed By: R. Walker
Case #24CV429673
Envelope: 15922143**

TO: FILE COPY

RE: **23andMe Data Breach Cases**
CASE NUMBER: **JCCP5315¹**

RE: **Wilkus, et al. v. 23andMe, Inc.**
CASE NUMBER: **24CV429673**

NOTICE OF RESCHEDULED CASE MANAGEMENT CONFERENCES

The Case Management Conferences for the above-entitled cases have been rescheduled (from July 18, 2024) and you are directed to appear in court on:

Date: October 31, 2024

At: 2:30 p.m.

In: Department 7

Location: Superior Court, 191 North First Street, San Jose, CA 95113.

A copy of the current Complex Civil Litigation Guidelines may be downloaded from the Court's website.

A single updated Joint Case Management Statement shall be filed by the parties no later than five (5) calendar days prior to the next scheduled Case Management Conference.

For further information, contact the Complex Civil Litigation Department, (408) 882-2286.

Date: July 12, 2024

Hon. Charles F. Adams
Judge of the Superior Court

If you, a party represented by you, or a witness to be called on behalf of that party need an accommodation under the American with Disabilities Act, please contact the Court Administrator's office at (408) 882-2700, or use the Court's TDD line, (408) 882-2690 or the Voice/TDD California Relay Service, (800) 735-2922.

¹ Included Actions: (1) Morgenstern v. 23ANDME Holding Co., et al., Superior Court of California, County of San Francisco, Case No. CGC-23-610816; (2) Vasquez v. 23ANDME, Inc., Superior Court of California, County of Santa Clara, Case No. 23CV424996; (3) **PENDING** Wilkus, et al. v. 23ANDME, Inc., Superior Court of California, County of Santa Clara, Case No. 24CV429673.